SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Borna Pozojević

VALIDACIJA SIGURNOSTI BEŽIČNE PRISTUPNE TOČKE S CILJEM SPRJEČAVANJA PRISTUPA OSJETLJIVIM INFORMACIJAMA

DIPLOMSKI RAD

Zagreb, 2018.

Sveučilište u Zagrebu
Fakultet prometnih znanosti

DIPLOMSKI RAD

VALIDACIJA SIGURNOSTI BEŽIČNE PRISTUPNE TOČKE S CILJEM SPRJEČAVANJA PRISTUPA OSJETLJIVIM INFORMACIJAMA

SECURITY VALIDATION OF WIRELESS ACCESS POINT WITH PURPOSE OF PREVENTING THE ACCESS TO SENSITIVE INFORMATION

Mentor: prof. dr. sc. Dragan Peraković

Student: Borna Pozojević
JMBAG: 0135214800

Zagreb, svibanj 2018.

Sažetak

Glavna prednost, a istovremeno i značajan sigurnosni nedostatak bežičnih lokalnih računalnih mreža, je činjenica da se područje pokrivanja ne može kontrolirati kao i u žičanoj infrastrukturi. Standard za bežičnu komunikaciju naziva IEEE 802.11, omogućuje pristup mreži informacijsko komunikacijskog sustava čak i izvan područja zgrade ili objekta u kojoj se ona koristi. Povezivanjem na bežičnu infrastrukturu, napadaču je omogućeno daljnje napredovanje kroz sustav i ugrožavanje osjetljivih informacija koje on sadrži. Validacija sigurnosti informacijsko komunikacijskog sustava, jedan je od načina provjere implementiranih mjera zaštite u sustavu. Poznat još i kao penetracijsko testiranje, postupak je autoriziranog napada na sustav od strane izvođača testa. U radu je analiziran postupak penetracijskog testiranja informacijsko komunikacijskog sustava, napadom na uređaje u bežičnoj mreži fakulteta te je istraženo kojim informacijama i podacima je moguće pristupiti uporabom raznih alata iz Kali Linux operativnog sustava.

KLJUČNE RIJEČI: 802.11; sigurnost informacijsko komunikacijskih sustava; penetracijsko testiranje; osjetljive informacije

Summary

The main advantage, and a huge security vulnerability in the wireless network communication standard 802.11, is the fact that network coverage area can't be controlled as in its wired counterpart. This kind of networks can be accessed outside of the area or the building where the network is used, and after that the entire system can be compromised by an attacker in case there are no implemented security controls. Security validation of information and communication systems, also known as penetration testing, is security check of safety measures implemented in the system. It is a simulation of authorized attack performed by a tester who uses tools and thinks like an attacker. This paper analyzes the procedure of penetration testing of the faculty's information system that includes wireless network. The paper describes some possible attacks on other devices in the wireless network and investigates which sensitive information and data that can be acquired, by using various tools from Kali Linux operating system.

KEYWORDS: 802.11; information and communication systems security; penetration testing; sensitive information

SADRŽAJ

1. UVOD

U današnje vrijeme, veliki broj različitih informacijsko komunikacijskih (IK) sustava, kao dio svojeg mrežnog elementa, koristi bežične lokalne računalne mreže. One danas nalaze primjenu u velikom broju okruženja: od raznih ministarstava te vladinih organizacija i udruga, preko obrazovnih i sveučilišnih ustanova, također sve modernija postaje primjena u bolnicama i raznim zdravstvenim ustanovama. Uz višegodišnju primjenu u sektorima poput bankarstva i ostalim poslovnim sustavima poput različitih ugostiteljskih objekata, ova tehnologija postaje i nezaobilazni dio skoro svakog prosječnog kućanstva.

Iako donose mnoge prednosti, u odnosu na sada već tradicionalne žičane mreže, negativna strana je da one zbog primjene radio valova kao medija prijenosa, nekontrolirano proširuju područje pokrivanja signalom te time olakšavaju izvođenje napada na IK sustav. Razni oblici napada na ovakav tip mrežne komunikacije omogućuju napadaču neovlašten pristup IK sustavu, preko kojeg može uzrokovati štetu ili doći do raznih osjetljivih informacija i podataka koje se u njemu nalaze.

Jedno od područja informacijske sigurnosti, naziva sigurnost IK sustava, bavi se proučavanjem sigurnosnih izazova i donošenjem preporuka i mjera zaštite ovakvih sustava. Nekad su se izrazi poput informacijske sigurnosti i sigurnosti IK sustava, posebno zaštite njenog komunikacijskog tj. mrežnog dijela, mogli smatrati sinonimima jer se na mrežu gledalo kao na zaštitni zid koji je osiguravao ostatak sustava. Međutim danas to više nije moguće, zato što postoji previše ulaznih točaka koje su podložne iskorištavanju sa svrhom zaobilaženja sigurnosnih mjera mreže te omogućuju napad na sustav.

Validacija sigurnosti IK sustava je oblik provjere korištenih mehanizama i mjera zaštite IK sustava. Penetracijsko testiranje još je jedan od naziva za ovaj postupak, kojim se na legalan i autoriziran način identificiraju prijetnje i iskorištavaju otkrivene ranjivosti promatranog sustava. Ranjivosti se otkrivaju tijekom jedne od nekoliko faza ovoga postupka s ciljem unaprjeđenja razine sigurnosti IK sustava. Osoba koja provodi penetracijsko testiranje poznata je pod nazivom etički haker. Tijekom postupka validacije oni oponašaju potencijalne napadače te koriste slične alate i način razmišljanja. Ovakav način testiranja sustava služi kao mjera prevencije neovlaštenog upada u IK sustav, zato što ukazuje na sigurnosne propuste i nedostatke koji mogu biti iskorišteni kako bi se uzrokovala šteta.

Svrha rada je unaprijediti znanja i osnovne vještine iz informacijske sigurnosti, točnije iz područja koje se bavi sigurnosti IK sustava. Naglasak u radu je na provedbi validacije sigurnosti bežične pristupne točke. Uz navedeno prikazat će se klasifikacija prikupljenih informacija te dati prijedlozi za povećanje razine sigurnosti u bežičnim lokalnim mrežama.

Cilj ovog diplomskog rada je istražiti kojim je sve podacima i osjetljivim informacijama moguće pristupiti nakon povezivanja na bežičnu pristupnu točku u „Laboratoriju za sigurnost i forenzičku analizu informacijsko komunikacijskog sustava“ na Fakultetu prometnih znanosti, Sveučilišta u Zagrebu.

Rad je podijeljen u sedam tematskih cjelina:

1. Uvod
2. Sigurnost IK sustava
3. Standardizacija bežične lokalne mreže
4. Metodologija validacije sigurnosti bežične pristupne točke
5. Provedba validacije sigurnosti bežične pristupne točke u laboratorijskom okruženju
6. Analiza dobivenih rezultata i prijedlozi unaprjeđenja zaštite
7. Zaključak

Drugo poglavlje definira pojam sigurnosti IK sustava, jednog dijela područja informacijske sigurnosti. Opisuje čimbenike i bitne pojmove za razumijevanje problematike ovog područja informacijskih znanosti. Uz to definirani su pojmovi poput osjetljive informacije i klasificiranog podatka te razlog klasifikacije istih unutar organizacije.

Kako bi se shvatio princip validacije sigurnosti, potrebno je poznavati temeljne pojmove računalnih mreža, žičnih i bežičnih, poput: razumijevanja ISO OSI protokolnog stoga, nekih bitnijih mrežnih protokola i poznavanje standarda za bežične lokalne računalne mreže 802.11. O navedenima se govori u trećem poglavlju uz prikaz opasnosti ovakvih mreža i opisa nekih mjera zaštite.

U četvrtom poglavlju rada, opisan je postupak validacije sigurnosti, objašnjena je problematika definiranja pojma, navedeni su dijelovi (faze) koje svaki penetracijski test sadrži te objašnjene vrste sigurnosnih procjena. Uz navedeno predstavljene su neke poznatije metode provođenja i strategije testiranja.

Peto poglavlje prikazuje praktičan primjer provedbe ovakvog testiranja u sigurnom okruženju u laboratoriju Fakulteta prometnih znanosti. Poglavlje prolazi kroz faze validacije sigurnosti te predstavlja neke alate iz palete Kali Linux operativnog sustava, koji se u njima koriste. Jedan od primjera pokazuje oblik napada na dostupan terminalni uređaj u bežičnoj mreži, temeljan na presretanju komunikacije između pristupne točke i korisnika mreže. Drugi dio iteracije testiranja proučava kojim informacijama je moguće pristupiti nakon povezivanja na pristupnu točku, s ciljem otkrivanja osjetljivih informacija o IK sustavu ili njegovim korisnicima.

Šesto poglavlje opisuje i komentira rezultate dobivene istraživanjem u laboratoriju, odnosno prikazuje klasificiranje informacija dobivenih prilikom testiranja sustava. Uz potencijalne pronađene ranjivosti, predloženi su neki oblici smanjenja istih te ostale mogućnosti povećanja razine zaštite u laboratoriju.

Rad završava zaključkom te popisom literature korištene za izradu rada, popisom najčešće korištenih kratica te slika i tablica u radu.

2. SIGURNOST IK SUSTAVA

Sigurnost IK sustava je jedno od područja kojima se bavi znanost, naziva informacijska sigurnost. Ovo područje bavi se sigurnosnim problemima i rješenjima u IK sustavima i njegovim elementima (hardver, softver, komunikacija, podaci, ljudski faktor i organizacijske metode). Detaljno proučava razne vrste napada kojima sustav može biti izložen te donosi preporuke i smjernice za njihovo rješavanje. Pridržavanje istih ne znači da je sustav u potpunosti siguran, nego se koriste s ciljem smanjenja vjerojatnosti iskorištavanja prethodno otkrivenih i dokumentiranih ranjivosti IK sustava.

Nekad su se izrazi poput informacijske sigurnosti i sigurnosti IK sustava, posebno zaštite njenog komunikacijskog tj. mrežnog (*Network*) dijela, mogli smatrati sinonimima. Razlog tome je što se na mrežu gledalo kao na zaštitni zid koji je osiguravao klijentska računala sustava (terminalni uređaji računalne mreže). Sigurno konfigurirana mreža mogla je odbiti napadače od unutarnjih računala sustava [1].

S vremenom se to pokazalo nedovoljnim iz razloga postojanja previše ulaznih točaka koje su se koristile u svrhu zaobilaženja sigurnosnih mjera mreže te su omogućile napad na sustav. Primjeri su korištenje prijenosnih memorija od strane nesvjesnog korisnika i iskorištavanje određenih mrežnih protokola od strane zlonamjernih programa ili napadača, koje nije moguće detektirati ili blokirati sigurnosnim uređajima IK sustava.

To ne znači da je aspekt mrežne sigurnosti unutar IK sustava nebitan. Osigurana računalna mreža je osnova u postizanju sigurnosti IK sustava. Uz navedeno, neke aplikacije su smišljene i napisane tako da sigurnost prilikom komunikacije zahtijevaju od same mreže. Jedan od prioriteta organizacije u postupku zaštite informacija je svakako i povećanje mrežne sigurnosti IK sustava.

2.1. Izazovi u održavanju sigurnosti IK sustava

Izazov održavanja sigurnosti IK sustava, posebno njegovog komunikacijskog i mrežnog dijela, u stanju sigurnosti nikada nije bio veći. Razlog tome nisu samo potencijalni napadi nego i brojne poteškoće koje se susreću prilikom obrane od tih napada. Poteškoće su po [1], sljedeće:

Univerzalno spojeni uređaji – danas je nezamisliva situacija da bilo koji uređaj s komunikacijskom tehnologijom (stolno računalo, pametni telefon, pametni sat i drugo) nije spojen na internet. Iako ovo pruža razne prednosti, također olakšava napad na određeni uređaj.

Povećane brzine napada – s dostupnim modernim alatima, napadači mogu brzo skenirati milijune uređaja kako bi našli slabosti te pokrenuli napade u kratkom roku.

Sofisticiraniji napadi – napadi postaju sve kompleksniji stoga ih je sve teže otkriti i obraniti se od njih. Napadači danas koriste standardne internetske protokole i aplikacije kako bi izvršili napade koji se sve teže razlikuju od legitimnog mrežnog prometa. Drugi alati za napad mijenjaju svoje ponašanje kako bi napad učinili svaki put različitim, čime se dodatno komplicira njihovo otkrivanje.

Dostupnost i jednostavnost alata za napad – današnji softverski alati za napad ne zahtijevaju nikakvo sofisticirano znanje za uporabu. Veliki broj dostupnih alata sadrži grafičko korisničko sučelje (*graphical user interface*, GUI) koje olakšava uporabu ovakvih programa. Dio alata je potpuno besplatan i jednostavno dostupan korisnicima a najpoznatiji primjer je operativni sustav (OS) Kali Linux koji će se koristiti u praktičnom dijelu ovog rada.

Brže otkrivanje ranjivosti – slabosti u hardveru i softveru mogu biti relativno brzo otkrivene te iskorištene s novim alatima i tehnikama.

Kašnjenje sigurnosnih ažuriranja – proizvođači hardvera i softvera imaju konstantnu potrebu ažuriranja svojih proizvoda kako bi ih zaštitili od napada. Jedan antivirusni sigurnosni institut dnevno dobiva preko 200,000 podnesenih potencijalnih oblika zlonamjernog softvera. Zbog brzine pristizanja, proizvođači sigurnosnog softvera uvelike kasne s izdavanjem sigurnosnih nadopuna te idu u korist poteškoćama koje se javljaju u obrani IK sustava.

Slaba distribucija sigurnosnih ažuriranja – Dok veći proizvođači popularnih proizvoda, poput Microsofta, Applea i Adobea, imaju sustave koji redovito obavještavaju korisnike o sigurnosnim nadopunama za njihove proizvode, mali je broj proizvođača koji su također uložili novac u takve skupe sustave za distribuciju. Korisnici često ni ne znaju da su nadogradnje dostupne jer ne postoji pouzdano sredstvo obavijesti. Često se dogodi da proizvođač ni ne napravi sigurnosno ažuriranje koje rješava postojeći problem u softveru, nego izradi novu verziju programa koji zatim naplaćuje korisniku. Napadači se danas sve više usmjeravaju u otkrivanje i iskorištavanje ranjivosti u ovakvim proizvodima.

Distribuirani napadi – napadač može iskoristiti stotine tisuća računala nad kojima ima kontrolu u napadu na poslužitelj ili mrežu. Ovaj pristup "više protiv jednog" doslovno onemogućuje sprječavanje napada identificiranjem i blokiranjem jednog izvora.

Uvođenje mogućnosti donošenje vlastitog uređaja (*Bring Your Own Device*, BYOD) – do nedavno informatički odjeli tvrtki su bili "apsolutistički" te su samo oni određivali standarde tehnologija i uređaje koje su korisnici mogli koristiti unutar korporacijske mreže. Međutim početkom 2010. pojavom intenzivnog korištenja tablet računala i pametnih telefona, zaposlenici su počeli zahtijevati pristup toj mreži preko vlastitih uređaja. Ovaj trend omogućuje zaposleniku korištenje vlastitog uređaja kako bi se spojio na korporativnu mrežu te uzrokuje veliki problem IT odjelu jer je teško pružiti adekvatnu sigurnost, beskrajnom nizu uređaja koje tvrtka ne posjeduje.

Zbunjenost korisnika – korisnika se sve više tjera da donese teške sigurnosne odluke u vezi vlastitog računalnog sustava, ponekad s malo ili nimalo informacija koje bi im pomogle u odabiru. Nije neuobičajeno da se korisnika pitaju sigurnosna pitanja poput "Želite li pregledavati samo sadržaj koji je dostavljen sigurno?", "Je li sigurno staviti ovaj privitak u karantenu?" ili "Želite li instalirati ovaj dodatak?". S malo ili nimalo detalja i uputa, korisnici su natjerani pružiti odgovor na pitanje bez da razumiju sigurnosni rizik koji donose.

2.2. Informacijska sigurnost

Izraz informacijska sigurnost često se koristi kako bi se opisali postupci potrebni za osiguravanje informacije koja se nalazi u digitalnom obliku. Ovakvom informacijom upravlja mikroprocesor (poput onog na osobnom računalu korisnika), ista se nalazi na uređaju za pohranu podataka (tvrdi disk ili vanjska memorija) te se odašilje mrežom, poput lokalne računalne mreže (*Local Area Connection*, LAN) ili interneta [1].

Ciljevi informacijske sigurnosti su osigurati ispravno implementiranje zaštitnih mjera, koje su sposobne pretrpjeti potencijalne napade i spriječiti potpuni kolaps IK sustava u slučaju da se napad dogodi.

Informacijska sigurnost je postupak ili proces, pomoću kojeg podatak/informacija tijekom cijelog vremena svojeg postojanja, zadržavaju svojstvo povjerljivosti, cjelovitosti i dostupnosti svim autoriziranim osobama, koje ju imaju potrebu koristiti.

Ona je namijenjena zaštiti informacija koje pružaju neku vrijednost, određenim ljudima i organizacijama. Postoje ključni čimbenici informacijske sigurnosti, koji također moraju biti osigurani u ovom procesu, a to su povjerljivost, cjelovitost i dostupnost informacije.

Ova, bolje rečeno načela informacijske sigurnosti, obuhvaćena su pod zajedničkim terminom „CIA model “, po [1] i [2]:

- Povjerljivost (*Confidentiality*)

  Povjerljivost je osobina sustava koja osigurava otkrivanje informacija i podataka isključivo za njih autoriziranim osobama (entitetima ili procesima), u definirano vrijeme i s točno definiranom procedurom. Održavanje povjerljivosti sustava važno je kako bi povjerljive informacije u IK sustavu određene organizacije ostale zaštićene. Razina povjerljivosti u kojoj se podatak nalazi, mora ostati ista tijekom boravka podatka u IK sustavu i uređajima na kojima se nalazi u mreži, za vrijeme prijenosa mrežom te na odredištu.

- Cjelovitost (*Integrity*)

  Informacija ima vrijednost samo kada je potpuna, odnosno nije mijenjana ili je na nju utjecao neovlašteni korisnik. Cjelovitost IK sustava podrazumijeva zaštitu informacija od namjerne ili slučajne, ali neovlaštene modifikacije uzrokovane ljudskim utjecajem ili pogreškom u radu sustava. Elementi sustava poput hardvera, softvera i komunikacijskih mehanizama, moraju raditi usklađeno kako bi uspješno prihvatili i obradili podatke te ih prenijeli namijenjenim odredištima bez neočekivanih izmjena.

- Dostupnost (*Availability*)

  Uz točnost, vrijednost informacije ovisi i o njezinoj dostupnosti. Dostupnost se odnosi na raspoloživost tražene informacije ovlaštenim korisnicima u određenom trenutku i prema zadanim uvjetima, što uključuje uvjete povjerljivosti i integriteta. Ako ti uvjeti nisu ispunjenu tada njegova primarna funkcija gubi značaj odnosno nije moguće ispuniti zahtjeve

postavljene od krajnjih korisnika. Mrežni elementi, računala i aplikacije moraju pružiti potrebne funkcionalnosti za obavljanje predviđenih radnji uz prihvatljivu razinu izvedbe. Oni se također moraju moći oporaviti od svih nastalih smetnji na siguran i brz način kako bi se izbjegli nepovoljni utjecaji na produktivnost sustava.

U praktičnoj primjeni informacijske sigurnosti, često se događa da je ona usmjerena samo na održavanje povjerljivih informacija tajnom. Prijetnje cjelovitosti i dostupnosti, često su zanemarene te ih se razmatra nakon napada na IK sustava. Različite vrste organizacija zahtijevaju naglasak na pojedinom načelu sigurnosti. Nekima je najbitnija povjerljivost (poslovne tajne poduzeća), nekima je potrebna cjelovitost (iznosi financijskih transakcija) dok je nekima najbitnije očuvati dostupnost (*web* poslužitelji e-*commercea*) [2].

Iz navedenog se zaključuje da je informacijska sigurnost proces zaštite podataka/informacija koji se nalaze unutar IK sustava neke organizacije, te sve imovine potrebne za njegov ispravan rad. Za optimalnu učinkovitost u primjeni, proces informacijske sigurnosti potrebno je provoditi tijekom cijelog životnog ciklusa IK sustava, stoga on nikada ne može biti završen, osim u slučaju trajnog isključivanja sustava u kojem se provodi.

2.2.1. Područja informacijske sigurnosti

Definicija informacijska sigurnost uključuje i puno više od zaštite same informacije. Zato što se informacija nalazi na hardveru računala, određeni softver njome manipulira te se prenosi komunikacijskim medijima, svaki od ovih dijelova također mora biti zaštićen. Jedan od ciljeva informacijske sigurnosti je i očuvanje povjerljivosti, cjelovitosti i dostupnosti informacije na uređajima koji pohranjuju, upravljaju i odašilju informaciju [1].

Informacijska sigurnost kao pojam obuhvaća i mnoga područja vezana za problematiku sigurnosti i zaštite informacije, ta područja su po [2] i [3], sljedeća:

- Sigurnosna provjera – područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti koji se primjenjuju na osobe koje imaju pristup klasificiranim podacima.
- Fizička sigurnost – područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti za zaštitu objekta, prostora i uređaja u kojem se nalaze klasificirani podaci.
- Sigurnost podatka – je područje informacijske sigurnosti za koje se utvrđuju mjere i standardi informacijske sigurnosti koje se primjenjuju kao opće zaštitne mjere za prevenciju, otkrivanje i otklanjanje štete od gubitka ili neovlaštenog otkrivanja klasificiranih i neklasificiranih podataka.
- Sigurnost informacijskog sustava – područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti klasificiranog i neklasificiranog podatka koji se obrađuje, pohranjuje ili prenosi u informacijskom sustavu te zaštite cjelovitosti i raspoloživosti informacijskog sustava u procesu planiranja, projektiranja, izgradnje, uporabe, održavanja i prestanka rada informacijskog sustava.

- Sigurnost poslovne suradnje – područje informacijske sigurnosti u kojem se primjenjuju propisane mjere i standardi informacijske sigurnosti za provedbu natječaja ili ugovora s klasificiranom dokumentacijom koji obvezuju pravne i fizičke osobe.
- Operacijska sigurnost – fokusira se na osiguranje svojstva organizacije da izvrši svoje operativne aktivnosti bez prekida ili ugroze
- Komunikacijska sigurnost – uključuje zaštitu organizacijskih komunikacijskih medija, tehnologije i sadržaja te svojstvo korištenja tih sredstava da postigne organizacijske ciljeve
- Mrežna sigurnost – odnosi se na zaštitu organizacijskih podatkovnih mrežnih uređaja, veza i sadržaja i svojstvo korištenja te mreže za izvršavanje organizacijskih podatkovnih mrežnih funkcija.

2.2.2. Terminologija informacijske sigurnosti

Prilikom opisivanja problema informacijske sigurnosti bitno je razumjeti izraze koji se pojavljuju u definicijama, vidljive na slici 1. Ona prikazuje odnose između osnovnih pojmova i njihove utjecaje na sigurnost sustava. Neki od njih poput ranjivosti, prijetnje ili uzroka prijetnje, rizika, utjecaja te izloženosti, često se neispravno koriste te je potrebno razumjeti razlike i veze između njih, po [2]:

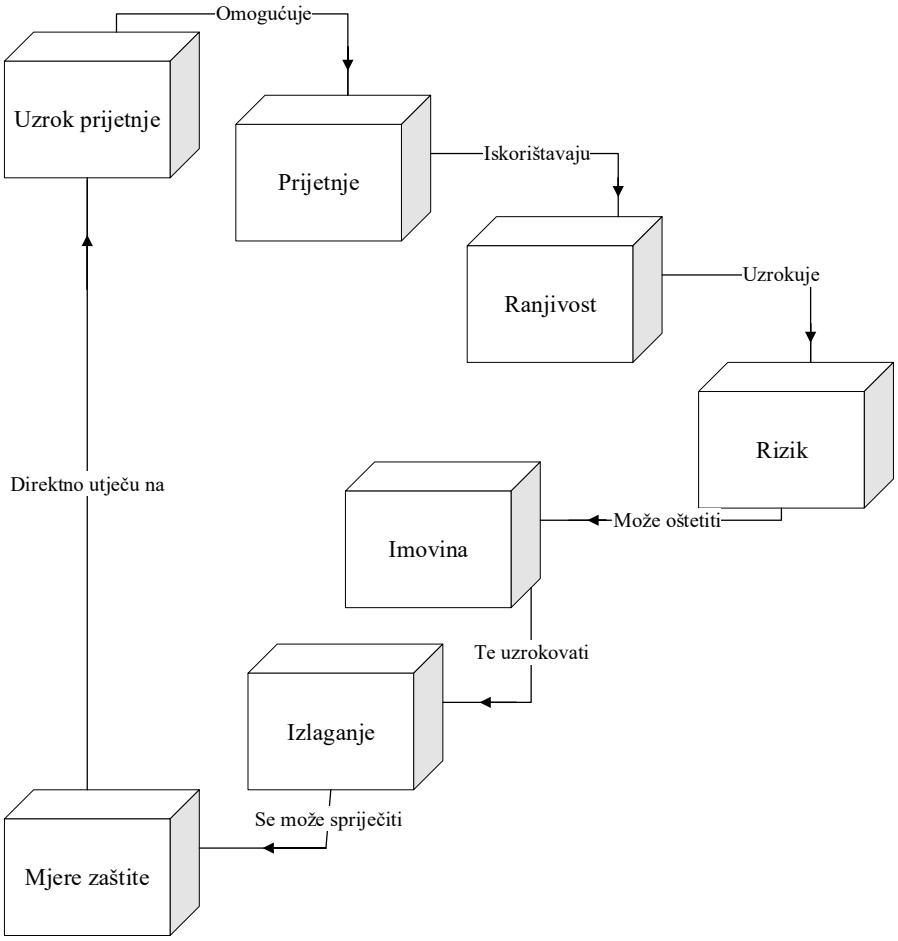
Entitet koji koristi ranjivosti sustava naziva se uzrokom prijetnje (*Threat agents*). Prijetnja (*Threat*) je potencijalna opasnost za sustav koja je povezana s iskorištavanjem (*Exploitation*) ranjivosti. Pojam prijetnje znači da će netko ili nešto, identificirati određenu ranjivost IK sustava te će istu upotrijebiti protiv njega ili bilo kojeg njegovog elementa, kako bi se uzrokovala šteta ili gubitak [1].

Ranjivost (*Vulnerability*) je nedostatak zaštitnih mjera ili propusti unutar zaštitnih mjera koje se provode u sustavu. Ranjivosti se mogu pojaviti u bilo kojem elementu IK sustava. Kad neka prijetnja iskoristi ranjivost sustava (*Exploit*), pojavljuje se mogućnost rizika koji utječe na imovinu.

Rizik (*Risk*) je funkcija vjerojatnosti da će uzrok prijetnje, iskoristiti određenu pronađenu ranjivost te odgovarajući poslovni utjecaj koji će događaj imati. Rizik povezuje ranjivost, prijetnju i vjerojatnost iskorištavanja koji rezultira odgovarajućim poslovnim utjecajem.

Imovina (*Asset*) predstavlja sve što ima neku vrijednost za organizaciju. Primjeri imovine su zgrade, uređaji, patenti, softver, financijska izvješća, usluge, ljudski resursi i drugo. Imovinu organizacije nemoguće je zamijeniti bez značajnih ulaganja resursa (financije, vrijeme, radna snaga ili drugih resursa) [1]. Oštećivanje imovine uzrokuje izlaganje sigurnosnom incidentu [2].

Izlaganje (*Exposure*) je situacija kada je sustav izložen gubitku ili šteti. Ranjivost izlaže organizaciju potencijalnom gubitku. U slučaju slabe provedbe usvojenih mjera o lozinkama, poduzeće se izlaže mogućnosti krađe korisničkih lozinki. Izlaganje sigurnosnom incidentu može se spriječiti korištenjem mjera zaštite.



Slika 1. Odnos između pojmova informacijske sigurnosti, izvor [2]

Mjere zaštite (*Countermeasure*) se postavljaju kako bi se smanjio potencijalni rizik. Mjere mogu biti postavke softvera, hardvera ili procedura koje uklanjaju vjerojatnost da će uzrok prijetnje uspjeti iskoristiti ranjivost. Neki od primjera mjera zaštite su jake lozinke, vatrozidi, zaštitno osoblje, mehanizmi kontrole pristupa i kriptiranje.

2.3. Osjetljive informacije i postupak klasifikacije

Osjetljive informacije (*Sensitive Information*) su svi podaci koji moraju biti zaštićeni od neovlaštenog pristupa kako bi se štitila privatnost i sigurnost pojedinca ili organizacije. Postoje tri glavne podjele ovakvih informacija [4]:

1. **Osobne informacije** (*Personal Information*) – su sve osjetljive informacije koje se mogu upotrijebiti sa svrhom identificiranja osobe te koje, u slučaju zlouporabe, mogu naštetiti toj osobi. Pod ove informacije pripadaju neke poput, prema [5]:

- Adresa fizičke osobe;
- Broj telefona;
- E-mail adresa;
- Osobna fotografija;

- Identifikacijski broj/OIB;
- Podaci o broju osobne iskaznice, vozačke dozvole ili registarskih oznaka
- Biometrijski podaci (otisak prsta, snimka šarenice oka);
- Podaci o obrazovanju i stručnoj spremi;
- Podaci o plaći, kreditnom zaduženju ili računima u banci.
- Rasno ili etničko podrijetlo
- Politička stajališta
- Vjerska ili druga uvjerenja
- Sindikalno članstvo
- Zdravlje ili spolni život
- Osobni podaci o kaznenom i prekršajnom postupku

2. **Poslovne informacije** (*Business information*) – osjetljive poslovne informacije uključuju sve što predstavlja rizik organizaciji o kojoj se radi u slučaju otkrivanja tih informacija od strane konkurenata ili opće javnosti. To uključuje:

- Poslovne tajne
- Planove nabave
- Financijske podatake
- Informacije o dobavljačima i klijentima te mnoge druge

> Poslovne informacije se pojavljuju u različitim oblicima poput: raznih izvješća, brošura, promotivnog materijala, internet stranica, javno dostupnih dokumenata preko mreže i sl. Svaki oblik poslovanja proizvodi nekih oblik zaštićenih informacija koje su povjerljive po prirodi te zahtijevaju određenu razinu zaštite od neprimjerenog ili nenamjernog otkrivanja. [6]

3. **Klasificirane informacije** (*Classified information*) - odnose se na državna tijela i ograničene su prema stupnju osjetljivosti.

2.3.1. Klasifikacija podataka od državnih tijela

Prema Zakonu o tajnosti podataka Republike Hrvatske [7], iznesene su definicije sljedećih pojmova:

*„**Klasificirani podatak** je onaj koji je nadležno tijelo, u propisanom postupku, takvim označilo i za koji je utvrđen stupanj tajnosti, kao i podatak kojeg je Republici Hrvatskoj tako označenog predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje,*

***Neklasificirani podatak** je podatak bez utvrđenog stupnja tajnosti, koji se koristi u službene svrhe, kao i podatak koji je Republici Hrvatskoj tako označenog predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje,*

***Klasifikacija podatka** je postupak utvrđivanja jednog od stupnjeva tajnosti podatka s obzirom na stupanj ugroze i područje ovim Zakonom zaštićenih vrijednosti,*

Deklasifikacija podatka *je postupak kojim se utvrđuje prestanak postojanja razloga zbog kojih je određeni podatak klasificiran odgovarajućim stupnjem tajnosti, nakon čega podatak postaje neklasificirani s ograničenom uporabom samo u službene svrhe. "*

Stupanj tajnosti pojedinom podatku određuje vlasnik podatka. Stupnjevi tajnosti su VRLO TAJNO, TAJNO, POVJERLJIVO i OGRANIČENO i ekvivalenti su stupnjeva tajnosti u engleskom jeziku: *TOP SECRET*, *SECRET*, *CONFIDENTIAL* i *RESTRICTED,* po [2] i [7].

- Stupnjem tajnosti VRLO TAJNO klasificiraju se podaci čijim bi neovlaštenim otkrivanjem nastala nepopravljiva šteta za nacionalnu sigurnosti i vitalne interese RH.
- Stupnjem tajnosti TAJNO klasificiraju se podaci čije bi neovlašteno otkrivanje teško naštetilo nacionalnoj sigurnosti i vitalnim interesima RH.
- Stupnjem tajnosti POVJERLJIVO klasificiraju se podaci čije bi neovlašteno otkrivanje naštetilo nacionalnoj sigurnosti i vitalnim interesima RH.
- Stupnjem tajnosti OGRANIČENO klasificiraju se podaci čije bi neovlašteno otkrivanje naštetilo djelovanju i izvršavanju zadaća državnih tijela u obustavljanju poslova u području nacionalne sigurnosti i vitalnih interesa RH.

2.3.2. Postupak klasificiranja podataka unutar organizacije

Važan aspekt unutar svake organizacije, koja koristi IK sustav, je prepoznavanje informacija koje su za nju ključne te dodjeljivanje vrijednosti istima. Razlog dodjeljivanja vrijednosti, različitim vrstama podataka/informacijama, je točna procjena potrebne količine novca i resursa koji će biti namijenjeni zaštiti svake vrste podatka (jer svaki podatak nema istu vrijednost za organizaciju). Nakon identificiranja svih bitnih informacija, iste trebaju biti propisno klasificirane. Svaka organizacija posjeduje mnogo informacija koje je stvorila i koje održava [2].

Razlog klasificiranja podatka je mogućnost organiziranja ovisno o osjetljivosti na gubitak, otkrivanje ili nedostupnost istog. Nakon segmentiranja po razini osjetljivosti, organizacija može odlučiti koje mjere su potrebne kako bi se zaštitile različite vrste podataka.

Ovime se osigurava potrebna razina zaštite informacijske imovine a klasifikacija pokazuje prioritet sigurnosne zaštite. Primarna svrha klasifikacije podataka je naznačiti razinu zaštite povjerljivosti, cjelovitosti i dostupnosti koja je potrebna za svaku vrstu skupine podataka. Klasifikacija podataka osigurava zaštitu podataka na najisplativiji način, te je potrebno trošiti novac na one informacije koje to stvarno zaslužuju.

Popis parametara kriterija koje organizacija može upotrijebiti kako bi utvrdila osjetljivost podataka je sljedeći [2]:

- korisnost i vrijednost podatka,
- starost podatka,
- razina štete koja bi se dogodila u slučaju otkrivanja podatka,
- razina štete koja bi se dogodila u slučaju modificiranja ili oštećivanja podatka,
- pravna, regulatorna ili ugovorena odgovornost za zaštitu podatka,

- učinak koji podatak ima na sigurnost,
- tko bi trebao pristupati podatku,
- tko bi trebao održavati podatke,
- tko bi trebao moći reproducirati podatke,
- izgubljeni troškovi prilika koji bi mogli nastati ako podaci nisu dostupni ili su oštećeni

Prilikom izrade klasifikacije, važno je ne pretjerivati ili napraviti dugi popis klasifikacija jer to može uzrokovati nejasnoće i frustracije pojedincima koji će ga koristi. Klasifikacije ne trebaju biti ni previše restriktivne nego dovoljno detaljne jer je potrebno klasificirati mnoge vrste podataka.

Svaka klasifikacija treba biti jedinstvena i odvojena od ostalih te između njih ne smije biti preklapanja. Proces klasifikacije također treba objasniti na koji način se informacije kontroliraju i kako njima barati kroz životni ciklus (od nastanka do brisanja). Nakon dovršetka sheme, potrebno je organizirati kriterije koji odlučuju o tome koja informacija pripada kojoj klasifikaciji.

2.3.3. Identifikacija osjetljivih informacija u IK sustavima

Za potrebe identificiranja osjetljivih informacija u IK sustavima, mogu se koristiti pitanja NERC (*North American Electric Reliability Corporation*), o zaštiti kritične infrastrukture (*Critical Infrastructure Protection*, CIP) [6]. Ista pomažu u identifikaciji potencijalnih osjetljivih informacija:

- Jesu li podaci ili informacije, odobreni od strane za to zaduženih i autoriziranih osoba, dostupni za javnu objavu?
- Sadrže li podaci ili informacije pojedinosti o ključnoj imovini tvrtke, ključnim objektima ili sustavima te sadrži li ranjivosti koje povećavaju potencijal mogućeg napada?
- Kada je riječ o kritičnoj imovini, ključnim objektima ili sustave tvrtke, sadrže li informacije detalje poput operativnih postupaka, topologije mreža ili sličnih dijagrama, tlocrte zgrada koje sadrže kritičnu opremu, planove za oporavak od katastrofe, planove reagiranja na incidente i sigurnosne informacije o konfiguracijama uređaja?
- Kakav utjecaj na kritičnu imovinu, ključne objekte IK sustava mogu imati informacije ako slučajno dođe do neželjenog otkrivanja istih?
- Sadrže li informacije osobne podatke koji identificiraju osoblje, kao što su podaci o biografiji, kontakt informacije, imena, adrese, telefonski brojevi, itd.?
- Kada bi netko namjeravao nanijeti štetu osoblju ili kritičnoj imovini i ključnim sadržajima, da li bi se informacija mogla koristiti u te svrhe?

Izvor [8], kao moguće osjetljive informacije koje se pojavljuju prilikom provođenja postupka validacije sigurnosti IK sustava, nabraja sljedeće:

- informacije povezane s elektroničkom imovinom unutar organizacije u kojoj se testiranje provodi
- informacije o aplikacijama koje se izrađuju unutar tvrtke
- parametri mrežne sigurnosti
- postojeće ranjivosti
- mrežni uređaji
- postavke poslužitelja

Razlog tome je završno tehničko izvješće, koje sadrži sve otkrivene ranjivosti, uspješno provedene napade, popis mrežne opreme i ostale informacije koje mogu biti iskorištene za provođenje stvarnog napada. Iz tog razloga, dio ovog rada će sadržavati anonimizirane slike ili zapise kako ne bi poslužio za otkrivanje informacija o fakultetu.

2.3.4. Osjetljive informacije korisnika na bežičnim mrežama

U današnje vrijeme, nije neobično da se povjerljivi podaci koriste i na internetu. Aktiviranje korisničkih računa za razne usluge, internet bankarstvo, pregledavanje elektroničke pošte (*Email*), samo su neki od primjera korištenja modernih tehnologija.

Ovakvo korištenje podataka preko tradicionalnih oblika računalnih mreža prilično je sigurno od zlonamjernih korisnika. Međutim, danas najveći sigurnosni problem predstavlja korištenje navedenih, preko nesigurne tj. ne zaštićene bežične lokalne mreže, najčešće putem javno dostupnih i besplatnih pristupnih točaka.

Po istraživanju tvrtke Norton [9], čak 60% ispitanih korisnika ima lažni osjećaj sigurnosti vezan za uporabu osjetljivih podataka preko ovog načina mrežne komunikacije. Također, isti su skloni upuštanju u razne sigurnosne rizike preko nezaštićenih bežičnih mreža, poput:

- Pristup osobnim i poslovnim *email* računima
- Pristup računima društvenih medija
- Dijeljenje slika i videa
- Provjera bankovnih računa te pristup financijskim informacijama
- Pristup drugim vrstama računa uz pomoć lozinke
- Dijeljenje planova putovanja ili informacijama o lokaciji
- Slanje poslovne dokumentacije
- Uporaba osobnih informacija (datum rođenja, OIB, adresa)
- Iznošenje detalja o kreditnim karticama (prilikom internet kupovine)

Među najvećim prijetnjama sigurnosti organizacije, upravo su one usmjerene protiv ljudi na vodećim razinama. Predsjednici uprava, direktori i viši šefovi, najčešće su ciljana meta prilikom napada izvan područja ureda matične organizacije. Razlog tome su činjenice da upravo oni imaju pristup povjerljivim i osjetljivim informacijama IK sustava, te često putuju (izlaganje nezaštićenim pristupnim točkama) i koriste se različitim terminalnim uređajima [10] i [11].

3. STANDARDIZACIJA BEŽIČNE LOKALNE MREŽE

Sigurnosne funkcije standardnih mrežnih elemenata IK sustava, poput preklopnika i usmjerivača, mogu se iskoristiti za postizanje određenog stupnja u osiguranju mrežne komunikacije te time povećati sigurnost IK sustava [1]. Klasifikacija ovih uređaja, odvija se po njihovim funkcijama u teorijskom načinu rada računalnih mreža, naziva referentni model za otvoreno povezivanje sustava (*Open system interconnection*, OSI).

To je skup specifikacija predloženih od strane Međunarodne organizacije za standardizaciju (*International Organization for Standardization*, ISO) 1978. godine, koji je nakon revizije 1983. godine u uporabi i danas. One opisuju način na koji dva, hardverski različita uređaja, mogu ostvariti međusobnu komunikaciju na računalnoj mreži.

U području mrežne sigurnosti, problemi se često opisuju po OSI slojevima, kako rješenje problema ne bi utjecalo na ostale slojeve. U provođenju validacije sigurnosti, korak skeniranja mreže može se provoditi po slojevima kako bi se odredile potencijalne mete napada prisutne u IK sustavu.

3.1. OSI model u sigurnosti IK sustava

Teorija načina rada računalnih mreža objašnjena je ISO-OSI modelom, koji prikazuje način na koji mrežni uređaj priprema podatak za uspješan prijenos preko mreže te proces koji se događa na odredištu [1].

Sljedeća dva potpoglavlja opisuju slojeve modela s pripadajućim funkcijama, te opise protokola i komunikacijskih *portova*, koji su nužni pojmovi u validaciji sigurnosti IK sustava. Uz navedeno bavi se i načinima otkrivanja mrežnih uređaja na pojedinom OSI sloju.

3.1.1. Slojevi i funkcije OSI modela

OSI model označen je sa sedam slojeva (*Layer*): aplikacijski, prezentacijski, sjednički, transportni, mrežni, podatkovni i fizički. Svaki od njih opisuje određenu mrežnu funkciju koju sloj izvršava u postupku prijenosa podataka (Tablica 1), uz to opisani su osnovni protokoli, standardi ili mediji koje sloj koristi. Za identificiranje potencijalnih problema u mreži, potrebno je znanje o funkcijama i osnovnim protokolima OSI slojeva.

Princip rada temeljen je na enkapsulaciji odnosno postupku dodavanja zaglavlja poruci prije prosljeđivanja svakom nižem sloju ispod aplikacijskog. Na odredišnoj strani svaki sloj uklanja zaglavlje prije nego ga proslijedi sloju iznad sebe, sve do aplikacijskog sloja kojem poruka stiže u formatu u kojem je i poslana. Ovaj postupak se također može koristiti i u osiguravanju komunikacijskog kanala odnosno kao metoda zaštite prijenosa informacija mrežom.

Tablica 1. Slojevi OSI modela, uz kratki opis, funkciju i osnovne protokole

Redni broj	Naziv sloja	Osnovni opis	Funkcija u OSI modelu	Protokoli, medij ili standardi
1.	Fizički sloj (*Physical Layer*)	Kodira bitove okvira podatkovnog sloja u električne signale koje šalje ili prima putem fizičkog medija	Bavi se kodiranjem i signalizacijom te prijenosom i prijemom podataka u mreži	bakrena žica (*Copper cable*), optički kabel (*Fiber*) i bežična veza (*Wireless*)
2.	Podatkovni sloj / sloj veze podatka (*Data Link Layer*, DLL)	Dijeli podatke u okvire (*frame*). Sastoji se od kontrole logičke poveznice (*Logical Link Control*, LLC) i pristupa prijenosom mediju (*Media Access Control*, MAC)	Bavi se fizičkim adresiranjem (MAC), tvorbom i ispravnim redoslijedom dostave okvira na odredište. Uz to obavještava više slojeve o pogreškama u prijenosu	*Address Resolution Protocol* (ARP), *Point-to-Point Protocol* (PPP), *Ethernet* i *Fiber Distributed Data Interface* (FDDI)
3.	Mrežni sloj (*Network Layer*)	Ovaj sloj zadužen je za odabir rute po kojoj paketi putuju mrežom od izvora do odredišta te adresiranje paketa koji se dostavljaju	Bavi se logičkim adresiranjem (IP), usmjeravanjem paketa kroz mrežu, fragmentaciju i defragmentaciju na odredištu	*Internet Control Message Protocol* (ICMP), *Routing Information Protocol* (RIP), *Open Shortest Path First* (OSPF)
4.	Prijenosni/transportni sloj (*Transport Layer*)	Zadužen je za točnu isporuku segmenata i *datagrama* s izvora na odredište. Osigurava isporuku podataka redom, bez dupliciranja, gubitaka ili pogrešaka	Pruža pouzdane i nepouzdane komunikacijske usluge, otkriva i ispravlja greške u prijenosu te kontrolira protok informacija	*Transmission Control Protocol* (TCP), *User Datagram Protocol* (UDP) i *Sequenced Packet Exchange* (SPX)
5.	Sjednički sloj/ sloj sesije (*Session Layer*)	Kada dvije aplikacije trebaju komunicirati ili izmjenjivati podatke u mreži, potrebno je uspostaviti vezu između njih	Sloj sesije omogućava uređajima uspostavu, održavanje i raskid veze tj. sesije između aplikacija koje koriste	*Structured Query Language* (SQL), *Network File System* (NFS), *Network Basic Input/Output System* (NetBIOS)
6.	Prezentacijski sloj (*presentation layer*)	Bavi se sintaksom i formatom podatka. Prima podatke od aplikacijskih protokola	Prevoditelj koji format aplikacije prevodi u standardni format za prijenos podataka	*Graphic Interchange Format* (GIF), *Musical Instrument Digital Interface* (MIDI)

		te ih stavlja u oblik podržan u OSI modelu	mrežom. Bavi se kompresijom.	
7.	Aplikacijski sloj (*Application Layer*)	Ovaj sloj omogućava GUI koji nudi mrežne usluge ili servisa (dostupni aplikacijama u računalnoj mreži)	Pruža usluge (*YouTube*, *RealTime Audio/Video*, prijenos datoteka, *email*, *web* stranice) za aplikacije	*File Transfer* (FTP) *Hypertext Transfer* (HTTP) i *Simple Mail Transfer Protocol* (SMTP)

Izvor : [1], [2], [12] i [13]

Podaci putuju slojevima OSI modela točno određenim redoslijedom. Aplikacijski sloj može komunicirati samo s aplikacijskim slojem drugog računala, dok na istom računalu on prosljeđuje podatke samo prezentacijskom sloju. Prilikom slanja dokumenta preko mreže, dokument uvijek prolazi put od aplikacijskog sloja preko ostalih sve do fizičkog, a na računalu koje prima podatak put će ići od fizičkog preko podatkovnog, mrežnog i transportnog sloja pa do aplikacijskog [2].

3.1.2. Uloga protokola i komunikacijskog *porta* u provedbi sigurnosti

Mrežni protokol (*Network protocol*) je standardizirani skup pravila koji određuju način razmjene podataka preko mreže. Dva različita uređaja, koristeći isti mrežni protokol, mogu komunicirati i razumjeti se [2]. Oni su osnova rada svake mreže i bez njih komunikacija između različitih uređaja ne bi bila moguća [12].

Unutar podatkovnog paketa transportnog sloja, postoji definirana identifikacija procesa ili usluge kojem se pristupa na višem sloju prilikom komunikacije. *Port* je 16 bitni podatak zapisan u zaglavlju TCP i UDP paketa, koji identificira pokrenutu mrežnu uslugu ili aplikaciju [12]. Jednostavnije rečeno, portovi pružaju put ili lokaciju na kojoj softver, usluga ili mreža obavlja komunikaciju s hardverom računala. [14].

S obzirom na to da je komunikacija na mreži raznolika i da računalo koje sudjeluje u mreži obavlja više procesa odjednom, na transportnom sloju definiraju se vrata (*Socket*) [12]. *Socket* čine IP adresa i oznaka TCP/UDP *porta* koji tako identificira procese za aplikacijski sloj. Transportni sloj kroz *socket* prosljeđuje podatke procesu, koji se nalazi na aplikacijskom sloju te omogućava komunikaciju između dva računala [13].

3.2. Otkrivanje dostupnih uređaja IK sustava pomoću nižih OSI slojeva

Razlog potrebe poznavanja OSI modela je činjenica da se napad u IK sustavu odvija po navedenim slojevima. Za potrebe ovog rada glavna tri sloja su sloj veze podatka, mreže i transporta koji pripadaju u niže slojeve OSI modela.

Oni se koriste za uspješan transport mrežnog prometa s izvora na odredište. Mnogi protokoli ovih slojeva zahtijevaju odgovor od odredišnog računala te se mogu iskoristiti za identifikaciju sustava koji se trenutno nalaze aktivni na mreži. Opis otkrivanja po pojedinom sloju nalazi se u sljedećim potpoglavljima.

3.2.1. Otkrivanje mrežnih uređaja na sloju veze podatka

Otkrivanje mreže (*Network discovery*) na drugom OSI sloju, provodi se pomoću protokola za razrješavanje adrese (ARP). On služi za prevođenje logičke IP adrese u fizičku MAC adresu. Kada računalo treba identificirati MAC adresu koja odgovara logičkoj adresi drugog uređaja, ono odašilje paket s ARP zahtjevom (*Request*) na lokalnom mrežnom segmentu. Uređaj s traženom IP adresom odgovara na zahtjev ARP odgovorom (*Reply*) koji sadrži MAC adresu. Računalo koje je poslalo zahtjev, adresu sprema u svoju ARP predmemoriju (*Cache*) koja je privremeni zapis svih IP i MAC adresa s kojima komunicira. Nakon toga pokreće komunikaciju s mrežnim uređajem (*Network Host*) [15].

Ovaj protokol je koristan u otkrivanju dostupnih uređaja na mreži, jer ne zahtijeva nikakav oblik identifikacije ili autorizacije prije odgovora na zahtjev. Postupak mrežnog nabrajanja (*Network enumeration*) obavlja se tako da se pošalje niz ARP zahtjeva kako bi se dobio popis korištenih IP adresa.

Prednosti ovakvog načina otkrivanja uređaja dostupnih na mreži su brzina i pouzdanost dobivenih rezultata, dok se nedostaci očituju u činjenici da je otkrivanje moguće samo u lokalnoj podmreži u kojoj se zahtjev šalje.

3.2.2. Otkrivanje mrežnih uređaja na mrežnom sloju

Najpoznatiji i najčešće korišten način otkrivanja *hostova* je otkrivanje na trećem sloju. Ovdje je riječ o tzv. *ping* (*packet internet groper*) naredbi, koja koristi protokol za kontrolu internet poruka (ICMP) [15].

Njegove funkcije, odnosno poruke *echo* zahtjev (*Request*) i *echo* odaziv (*Reply*), koriste se za identificiranje trenutno spojenih uređaja na mrežu. ICMP *echo request* je upit kojim jedno računalo pita drugo "Jesi li ovdje?". ICMP *echo reply*, je odgovor drugog računala sa "Jesam, tu sam". Za otkrivanje mrežnog računala s određenom IP adresom, potrebno je poslati ICMP *echo request* na traženu adresu. Ako se računalo s traženom adresom nalazi na mreži i radi, isto odgovora u obliku ICMP *echo reply* [14].

Ovaj protokol koristi se za otkrivanje *hostova* dostupnih na mreži. Postupak se ponavlja za određeni raspon sve dok se ne dobije popis dostupnih IP adresa. Dobiveni popis sadrži sve IP adrese s kojih je zaprimljen odgovor [15].

Otkrivanje uređaja na trećem sloju je učinkovito zato što koristi rutirajući protokol za identifikaciju *hostova*. Nedostaci su brzina izvođenja jer je ICMP mnogo sporiji od ARP-a. Ovakav način otkrivanja manje je pouzdan nego otkrivanje pomoću ARP-a zbog konfiguriranja određenih uređaja da ne odgovaraju na ICPM zahtjeve. Vatrozidi (*Firewall*) su na primjer većinom konfigurirani da odbacuju ovakve pakete.

3.2.3. Otkrivanje mrežnih uređaja na transportnom sloju

Otkrivanje na četvrtom sloju OSI modela vrlo je učinkovito jer se javno rutirani sustavi (*Publicly Routable Systems*) nalaze samo u prostoru javnih IP adresa, budući da omogućuju mrežne usluge dostupne preko TCP-a ili UDP-a. U loše osiguranim okruženjima, odgovor (*Reply*) može biti potaknut od udaljenog poslužitelja (*Remote Server*) slanjem bilo kakvog UDP ili TCP zahtijeva (*Request*) na njegovu IP adresu. Korištenjem dinamičkog filtriranja (*Stateful Filtering*) u vatrozidu IK sustava, postoji šansa da se odgovor može dobiti od udaljene usluge samo uz pomoću SYN zahtjeva, usmjerenog na *port* adrese povezane s uslugom. U okruženjima s velikom razinom zaštite i naprednim filtriranjem, moguće je otkriti uređaje ako se postavi pravi zahtjev. Zbog postojanja 65,536 mogućih *portova* UDP i TCP usluga, potpun i detaljan process otkrivanja uređaja na mreži ovim putem može dugo trajati. Optimalan pristup otkrivanja uređaja na ovoj razini je ravnoteža između temeljitosti i svrsishodnosti pretrage [15].

Otkrivanje na četvrtom sloju pomoću TCP-a sastoji se od slanja TCP paketa na potencijalne odredišne adrese s aktiviranim bitovima raznih TCP zastavica (*Flag*). Različite postavke zastavica pokreću različite odgovore koji mogu biti iskorišteni za identifikaciju *hostova*. Namjera nije izazvati određeni odgovor nego bilo kakav odgovor jer je to potvrda da se sustav nalazi na mreži [14] i [15].

Otkrivanje pomoću UDP-a sastoji se od slanja UDP ispitnog paketa (*Probe*) na odredišne portove s ciljem izazivanja odgovora. Otkrivanje pomoću UDP-a može biti učinkovito prilikom identificiranja računala koja imaju filtrirane sve TCP usluge. Međutim, ovakav način otkrivanja može biti kompliciran zato što neke UDP usluge na zahtjev odgovaraju s ICMP odgovorom "*port* nedostupan" (*Port-unreachable*), dok druge odgovaraju samo na jedinstvene zahtjeve koji moraju odgovarati određenoj pokrenutoj usluzi. ICMP promet je često filtriran izlaznim ograničenjima vatrozida, čime se otežava ovakav način otkrivanja. Zbog toga, efektivno otkrivanje *hostova* pomoću UDP-a zahtjeva jedinstvene tehnike koje variraju od usluge do usluge.

3.3. Bežični standard IEEE 802.11

IEEE (*Institute of Electrical and Electronics Engineers*) je neprofitna stručna udruga i vodeći autoritet na širokom tehničkom području od računalnih znanosti, biomedicinske tehnike i telekomunikacija, preko električne energije, potrošačke elektronike do mnogih drugih područja [16].

Unutar organizacije IEEE formirana je radna skupina kako bi se izradila specifikacija za bežične lokalne mreže. Taj projekt polako je prerastao u obitelj specifikacija za bežične lokalne računalne mreže (*Wireless Local Area Network,* WLAN) imena IEEE 802.11. To su specifikacije iz područja kontrole pristupa mediju (MAC) i fizičkog sloja koje upravljaju komunikacijom u bežičnim mrežama frekventnih opsega od 2,4 do 5 GHz [17].

3.3.1. Specifikacije 802.11. standarda

O standardu su napisane mnoge specifikacije prikazane u tablici 2. Svaki je označen identificirajućim slovom a osim godine ratifikacije navedeni su i pripadajući radio frekvencijski (RF) opsezi odnosno područja rada standarda. Od drugih bitnih značajki važno je naglasiti teoretsku brzinu fizičkog sloja te razinu sigurnosti koju standard pruža.

Tablica 2. Standardi 802.11 s pripadajućom oznakom, opisom i sigurnosnom razinom uz značajke poput opsega i teoretske brzine prijenosa

Oznaka	Godina	RF opseg	Brzina	Opis standarda	Razina sigurnosti
802.11	1997.	2,4 GHz	1 – 2 Mbit/s	Prva specifikacija za WLAN	Slaba – tehnike filtriranja MAC adresa uz prve oblike WEP-a
802.11a	1999.	5 GHz	Do 54 Mbit/s	Proširenje 802.11 koje donosi 23 kom. kanala koja se ne preklapaju	Slaba – kao i kod 802.11 b
802.11 b, Wi-Fi	1999.	2,4 GHz	11 Mbit/s	Nudi funkcionalnosti WLAN-a sličnu razini *Ethernet* mreža	Slaba – uporaba WEP-a. 2001. prvo probijanje WEP 64 bitnog ključa
802.11 g	2003.	2,4 GHz	54 Mbit/s	Također vrlo popularna specifikacija kod proizvođača opreme i korisnika	Umjerena – WPA ublažio nedostatke i povećao razinu sigurnosti. Koristi 128 bitni ključ
802.11 i	2004.	GHz	/	Implementiran kao WPA2 sigurnosni algoritam tj enkripcijski standard	Srednja – koristi AES/CCMP enkripciju te povećava sigurnost mreže. Ugrožen 2017. i pojavom KRACK napada
802.11 e	2005.	GHz	/	Unaprjeđuje 802.11 a i b. Donosi mogućnost kvalitete usluge (QoS)	Srednja – omogućuje uporabu VLAN-a u WLAN-u
802.11/ WPS	2007.	GHz	/	Certifikat Wifi Alijanse koji umjesto uporabe WPA ili WPA2 lozinke koristi brojčani WPS PIN	Slaba – uporaba 8 znamenkastih lozinki, zahtijeva kraće vrijeme probijanja WPS PIN-a od probijanja WPA2 lozinke

802.11 w	2009.	GHz	/	Standard za zaštitu nekih upravljačkih okvira (*Management frames*) u WLAN-u	Srednja – Nadopuna 802.11i kojim se u prijenosu štite podatkovni okviri te povećava razina zaštite
802.11 n	2009.	2,4 i 5 GHz	600 Mbit/s	Rad u dva frekvencijska opsega, maksimalne performanse u 5 GHz načinu rada	Srednja – koristi WPA2 uz mogućnost korištenja 802.1X za autentikaciju temeljem porta
Novi 802.11 X	2018.	GHz	/	Početkom 2018. i najavom WPA3 sigurnosnog protokola siguran je dolazak i odgovarajućeg 802.11 amandmana	Visoka – očekuju se rješenja problema prethodnika. Povećanje sigurnost u otvorenim mrežama uz OWE enkripciju

izvor [17], [18], [19], [20], [21], [22], [23] i [24]

Iz tablice je vidljiv razvoj standarda u dvadeset godina, te danas postoje razni oblici narušavanja njegove sigurnosti prilikom korištenja. Stoga je koncept njegovog osiguravanja od velike važnosti u području sigurnosti IK sustava.

3.3.2. Dijelovi bežične računalne mreže

Standardom IEEE 802.11 definirani su osnovni dijelovi WLAN-a pod koje spadaju sljedeći elementi, po [16] i [25]:

- Mrežna kartica (*network interface card, NIC*) – povezuje klijenta s pristupnom točkom
- Pristupna točka (*access point*, AP) – međusobno povezuje klijente te ih spaja na žičanu mrežnu infrastrukturu IK sustava
- Osnovni skup usluga (*Basic Service Set*, BSS) – sastoji se od dva ili više klijenta ili stanica, skraćeno STA (*station*). Svaki BSS ima svoju jedinstvenu oznaku BSSID (BSS *Identifier* = temeljen na MAC adresi AP-a)
- Područje pokrivanja bežičnog LAN-a unutar kojeg članovi BSS-a mogu međusobno komunicirati naziva se osnovno područje pružanja usluge (*Basic Service Area* – BSA) LAN koji se sastoji od samo jednog BSS-a naziva se IBSS (*Independent* BSS), što je IEEE-ov pandan neovisnom LAN-u
- Distribucijski sustav (*Distribution System* – DS) međusobno povezuje dva ili više BSS-a, koristeći pritom najčešće žičanu ili optičku mrežu
- Bežični LAN koji čine DS i njime povezani BSS-ovi, nazvan je prošireni skup usluga (*Extended Service Set* – ESS). Poput BSS-a, i ESS ima jedinstvenu oznaku ESSID (ESS *Identifier* = u Kali alatima odgovara imenu mreže)

3.4. Sigurnosni izazovi uporabe bežičnih mreža u IK sustavu

Slično LAN-u, i WLAN mreža je zapravo prostorno ograničena u pogledu postizanja kvalitetnog signala ali u svom dometu omogućuje komunikaciju računalima povezanima na nju. Osim računala za koja je mreža namijenjena, bez odgovarajućih mjera zaštite, na istu se može spojiti bilo koje računalo u dometu.

WLAN-om se koriste mnoge državne ustanove, fakulteti, velike korporacije, privatna poduzeća, ugostiteljsko uslužni objekti i prosječna kućanstva. Osim kvalificiranog osoblja, istoj pristupa i veliki dio ne dovoljno educiranih korisnika, koji zbog ranjivosti ovakvog načina komunikacije predstavljaju veliki izazov u očuvanju sigurnosti IK sustava.

Bežične mreže sigurnosno su više ugrožene od onih u kojima se podaci prenose putem žice zbog nekontroliranog prijenosa podataka u cijelom dometu pristupne točke ih te svatko tko se nalazi u blizini može pokušati presresti. Napadi na WLAN u IK sustavima mogu se iskoristiti i napad na računala u unutrašnjem, žičano povezanom dijelu mreže [22].

3.4.1. Zabilježeni napadi na osjetljive informacije u WLAN-u

Primjer napada na bežičnu mrežu opisuje izvor [26], u kojem opisuje prijetnje i napade na mreže korporacija te ukazuju na opasnosti upotrebe WLAN-a bez odgovarajućih mjera sigurnosti. U članku je naveden primjer lošeg osiguranja WLAN-a školskog okruga Palo Alto u Americi. Zbog slabo provedenih mjera sigurnosti, lokalna novinarska agencija uspjela je dobiti pristup osjetljivim informacijama polaznika škole poput ocjena, brojeva kućnog telefona i adrese, slika u boji te psiholoških procjena učenika.

Drugi slučaj neautoriziranog pristupa povjerljivim i osjetljivim informacijama [27], opisuje napad koji je krenuo nakon iskorištavanja slabosti WLAN-a kako bi ostvario pristup IK sustavu TJX, velikog američkog trgovačkog lanca odjeće. Napadači su s parkinga u blizini ulaza u trgovinu, uz pomoć antene hvatali bežične transakcije u dućanu. Ova je bilo moguće zbog toga što su se podaci odašiljali WLAN-om dućana koja nije bila zaštićena. To je napadačima omogućilo prisluškivanje mrežnog prometa bez potrebe otkrivanja svog identiteta ili namjene. U roku od dva dana uspjeli su zaobići mjere sigurnosti u obliku WEP ključa te proširiti obuhvat napada. Napadači su kroz dvije godine zadobili pristup centralnoj bazi podataka korisnika te su ugrozili 45 milijuna kreditnih kartica i omogućili krađu korisničkih podataka poput vozačkih dozvola, OIB-a i sl.

Izvor [11] analizira skup zloćudnih programa pod nazivom „*Darkhotel APT* “. Rad opisuje napade na istaknute zaposlenike svjetskih kompanija koji su pristupali na zaražene WLAN mreže te tako nesvjesno odavali povjerljive poslovne informacije. Pristupne točke najčešće su se nalazile u elitnim hotelima diljem svijeta gdje su poslovno boravili. Mete napada bili su visoko pozicionirani zaposlenici tj. direktori, predsjednici i ostali važni članovi međunarodnih kompanija. Cilj napada bio je omogućiti pristup povjerljivim i osjetljivim informacijama zlonamjernim korisnicima. Zaraženi AP korisniku je predlagao instalaciju zlonamjernih programa, koji bi mu omogućili korištenje interneta pomoću AP-a.

3.4.2. Prijetnje i napadi na WLAN mreže IK sustava

Princip rada WLAN-a tj. uporaba RF za komunikaciju omogućuje različite napade. Isti su usmjereni na povredu načela sigurnosti. Osnovna podjela napada moguća je u pasivne i aktivne napade [25].

Pasivnim napadima pripadaju oni u kojima napadač pokušava zadobiti pristup informacijama ili podacima koji se prenose otvorenom mrežom. Otkrivanje ovakvih napada je dosta teško jer napadač ne utječe na sadržaj paketa. Podvrste ove kategorije su prisluškivanje kanala (*eavesdropping*) i analiza mrežnog prometa (*traffic analysis, sniffing*).

Napad prisluškivanja direktno utječe na povjerljivost podataka a napadaču omogućuje pristup mrežnom prometu te čitanje sadržaja poruka koje se odašilju kroz mrežu. Princip rada WLAN-a onemogućuje kontrolu nad radiovalovima te je komunikacija podložna prisluškivanju s udaljenih lokacija [28]. Prisluškivanjem kanala napadač može dobiti uvid u promet koji se odvija na mreži. Njegovom analizom mogu se saznati MAC adrese računala koje se koriste u lokalnoj mreži te se lažno predstaviti kao ovlašteni korisnik u mreži [22].

Analiza mrežnog prometa je jedan od prvih koraka u napadu na IK sustav. Tehnikom se određuje komunikacijsko opterećenje, broj odaslanih i prihvaćenih paketa, njihova veličina te izvor i odredište paketa. Pomoću analize prometa, napadač može skupiti tri oblika informacija o mreži: identifikaciju aktivnosti na mreži, broja pristupnih točaka i pripadajućih lokacija u okolini. Treći oblik informacije je upoznavanje s korištenim protokolima u mreži, odnosno veličinom, tipom i brojem paketa koji se kreću kroz nju [25].

Aktivnim napadima se smatraju oni u kojima napadač, osim pristupa informacijama u mreži, utječe na sadržaj tj. mijenja informaciju ili kreira potpuno lažne informacije na mreži. Pod neke od primjera aktivnih napada dostupnih u WLAN-u pripadaju, [22] i [25] :

- Neautorizirani pristup (*Unauthorized Access*) – napadaču je cilj zadobiti pristup cijeloj mreži kako bi mogao koristiti usluge i privilegije koje mu nisu dostupne. Određene arhitekture omogućuju pristup LAN-u preko WLAN-a.
- Lažna pristupna točka (*Rogue Access Point*) – napad zlonamjernim povezivanjem na mrežu te predstavljanje napadačeve mrežne kartice kao legitimne pristupne točke mreže. Posljedica uspješnog napada je ta da se sav mrežni promet te bežične mreže preusmjerava kroz napadačevo računalo.
- Napadi presretanjem komunikacije (*Man-in-the-middle, MITM*) – uspješnim izvođenjem napada zlonamjernog povezivanja, napadač može saznati osjetljive podatke koje zatim koristi za posredovanje u komunikaciji. Krajnji korisnici nesvjesni su da podatke šalju posredniku i primaju putem posrednika (koji se predstavlja kao pristupna točka)
- Napadi uskraćivanjem usluge (*Denial-of-Service*, DoS) – napadač pokušava spriječiti legitimnog korisnika da pristupi određenoj usluzi, računalu ili mreži. Načini na koji se postiže ovaj napad su preplavljivanje klijenta ili poslužitelja s lažnim paketima i zahtjevima, nevažećim porukama te dupliciranim IP ili MAC adresama i drugim.

3.5. Metode zaštite bežičnih mreža

U zaštiti bežičnih mreža mogu se koristiti djelomične metode za zaštitu od neovlaštenog pristupa kao što su statičko IP filtriranje ili filtriranje na razini MAC adresa. To nisu preporučene vrste zaštita zbog mogućnosti lažiranja IP i MAC adresa [22].

Optimalni oblik zaštite bežične mreže je uporaba posebno oblikovanih sigurnosnih protokola poput WEP, WPA i WPA2, dok će se u budućnosti koristiti tek najavljeni WPA3. U potpoglavljima koje slijede kratko su opisani i navedeni protokoli za sigurnost WLAN-a, u obliku četiri generacije metoda za zaštitu bežičnih mreža. Uz njih su opisane i ostale dostupne metode koje se preporučuju koristiti u svrhu povećavanja sigurnosti WLAN-a u IK sustavima.

3.5.1. Prva generacija metoda zaštite – WEP

WEP (*Wired Equivalent Privacy*) je protokol za zaštitu bežičnih mreža, opisan IEEE standardom 802.11. WEP zaštita odnosi se na fizički i sloj veze podatka u računalnoj mreži, a temelji se na enkripciji podataka između krajnjih točaka [22].

WEP koristi kriptografske ključeve duljine od najmanje 64 bita, koji se sastoje od ključa veličine 40 bita i inicijalizacijskog vektora (IV) od 24 bita. Optimalna duljina ključa je ona koja onemogućuje njegovo otkrivanje (što veća), a da se enkripcija istovremeno može obaviti što brže (što manja). Kriptiranje i dekriptiranje podatka obavlja se tajnim ključem u krajnjim točkama mreže, a protokol uključuje provjeru integriteta poruke i provjeru identiteta korisnika. Poznavanjem ključa moguće je upotrebom iste funkcije dekriptirati poruku na odredištu.

Prvi napad na WEP izveden je 2001. godine i tada je pokazano da se privatni ključ može, pomoću prisluškivanja mreže, otkriti za manje od nekoliko minuta. Napad je ubrzo nakon toga i programski izveden, a 2005. je pokazano da se za tri minute može ostvariti neovlašten pristup bilo kojoj mreži zaštićenoj WEP metodom i to uz pomoć javno dostupnih programskih alata [26].

Nakon što je dokazana nesigurnost WEP protokola, izašle su njegove poboljšane inačice: WEP2 koji ima povećane vrijednosti IV i ključa na 128 bita, WEP plus kod kojeg je povećana učinkovitost sprječavanjem korištenja loše oblikovanih IV-a koji se lako otkrivaju te D*ynamic* WEP koji dinamički mijenja ključeve [22].

Problem kod poboljšanih inačica WEP-a je taj što ih ne podržavaju svi proizvođači, nisu pogodne za izvedbu zbog velikog zahtjeva za procesnom snagom i ne omogućavaju zadovoljavajuću zaštitu (i dalje postoje metode koje više ili manje uspješno zaobilaze ovaj tip zaštite).

3.5.2. Druga generacija metoda zaštite – WPA

WPA (*Wi-Fi Protected Access*) je metoda zaštite originalno opisana prije IEEE 802.11i standarda. On omogućuje enkripciju podataka i provjeru identiteta korisnika. Koristi 128-bitni

ključ i 48-bitni IV a prednost nad WEP standardom je u korištenju TKIP protokola (*Temporal Key Integrity Protocol*), koji dinamički mijenja ključeve za vrijeme korištenja sustava.

Kombinacijom dugačkog IV i TKIP protokola sustav se može lagano obraniti od napada koji se koriste za otkrivanje ključa kod primjene WEP protokola [22] i [26]. TKIP koristi složenije funkcije za stvaranje niza bitova kojima se kriptira tekst. Tako je napadaču otežano otkrivanje tajnog ključa prisluškivanjem mrežnog prometa.

U studenom 2008. godine otkrivena je ranjivost TKIP protokola koju napadač može iskoristiti za otkrivanje niza bitova kojima se kriptira određeni paket. Napad je moguće izvesti samo na kratkim porukama većinom poznatog sadržaja kao što su ARP poruke. Posljedice uspješne zlouporabe mogu biti podmetanje lažnih ARP paketa legitimnom klijentu.

WPA i WPA2 protokoli mogu se koristiti u dva načina rada, po [22] i [28]:

1. PSK (*Pre-Shared Key*) – koristi prethodnu razmjenu ključeva između pristupne točke i svih klijenata. Pruža mnogo manju razinu sigurnosti nego poslovni oblik (*Enterprise*)

PSK način rada još se naziva i privatni (*Personal*) . On je namijenjen privatnim ili manjim poslovnim mrežama. Jednostavniji je za izvedbu od *Enterprise* sustava jer ne zahtijeva uporabu autentikacijskog poslužitelja, već se definira jedinstveni 256 bitni ključ (lozinka) koji se koristi za komunikaciju u mreži. Ključ se unosi kao 64 heksadecimalne znamenke ili niz od 8 do 63 ASCII znakova na temelju kojeg se računa ključ za enkripciju podataka. Budući da za 256 bitova postoji veliki broj mogućih kombinacija, ključ je nemoguće izračunati iz vrijednosti algoritma sažimanja (*hash*) u razumnom vremenu. Ako korisnik unese predvidljive nizove znakova, tada napadaču otkrivanje ključa može olakšati tzv. *brute force* napad koji podrazumijeva pretraživanje prostora svih mogućih kombinacija. Osim njega postoji i opasnost od napada rječnikom. Zbog toga je preporučena uporaba nelogičnih, nasumičnih nizova znakova prilikom stvaranja ključa.

2. *Enterprise* – podrazumijeva poseban ključ između pristupne točke i svakog klijenta.

Ovaj način rada pruža snažniju zaštitu jer autentikacija (identifikacija i potvrđivanja identiteta lozinkom) za potrebna svaki uređaj u mreži, no uvođenje i održavanje takvog sustava zahtijeva više posla. WPA *Enterprise* sadrži IEEE 802.1X standard koji pruža autenticirani pristup mreži, baziran na autentikaciji pristupa portova (*port-based authentication*). Za potrebe autentikacije klijenata uz AP koristi se i dodatni poslužitelj koji provodi postupak. WPA2 Enterprise autentifikacijski poslužitelji koriste RADIUS (*Remote Authentication Dial In User Service*) mrežni protokol za centraliziranu autentikaciju korisnika u IK sustavu.

3.5.3. Treća generacija metoda zaštite – WPA2

WPA2 se kao i WPA temelji na IEEE 802.11i standardu te uključuje sve njegove mehanizme uz uvedena dodatna poboljšanja poput CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) enkripcije. Sigurnosni dio IEEE specifikacije koji opisuje enkripciju i sigurnu komunikaciju među čvorovima u bežičnoj mreži naziva se i *Robust Security Network* (RSN) model [22].

Dio WPA2 protokola je EAP (*Extensible Authentication Protocol*), kojim se provodi međusobna autentikacija između klijenta i pristupne točke. EAP definira format poruka koje se izmjenjuju prilikom bežične autentikacije. Prilikom autentikacije u WPA2 protokolu izvodi se i razmjena ključeva pomoću kojih će se kriptirati podaci koji se šalju. WPA2 autentikacija izvodi se dinamičkim protokolom koji uključuje razmjenu u četiri koraka – svi potrebni podaci kojima se jamči sigurnost komunikacije razmjenjuju se u četiri poruke (*four way handshake).*

Kao odgovor na slabost TKIP enkripcije kod WPA protokola, WPA2 uvodi CCMP enkripciju koja se temelji na AES (*Advanced Encryption Standard*) algoritmu i ulančanom kriptiranju blokova. AES je simetričan kriptografski algoritam koji podatke kriptira po blokovima od 128 bita, a ključ kojim se kriptira može biti veličine 128, 192 ili 256 bita [26].

2007. godine *WiFi* Alijansa, predstavlja *WiFi Protected Setup* (WPS). On je zamišljen tako da korisnik, umjesto unosa znakovne lozinke WPA ili WPA2, za autentikaciju u mreži unese WPS PIN od 8 znamenki koji se nalazi na poleđini mrežnog usmjernika [1]. Iako je ideja bila široko prihvaćena, 2011. Stefan Viehböck objavljuje rad [23] koji opisuje ranjivosti i napad na WPS PIN. U njemu izlaže činjenicu da bilo koji PIN može biti otkriven u puno manjem vremenu nego što je to potrebno za probijanje WPA2 lozinke s istim brojem znakova. S vremenom se ovaj neuspjeli pokušaj zaštite prestao preporučivati kao sigurnosna mjera.

Enkripcija podataka u WLAN-u korištenjem WPA2 protokolom smatrala se sigurnom do 2017. godine i pojave napada nazvanog KRACK (*Key Reinstallation Attack*) [24]. Otkrivene ranjivosti koje se nalaze u jezgri WPA2 potencijalnom napadaču mogu pomoći ostvariti pristup WLAN-u koji omogućuje praćenje mrežne komunikacije. On je izazvao sigurnosni udar na bežične mreže zato što utječe na skoro sve bežične uređaje u IK sustavu. Napadom je moguće ugroziti i otkriti osjetljive informacije poput brojeva kreditnih kartica, lozinki, *e-mailova* i fotografija. Još jedan veliki problem je u činjenici da je u napadu riječ o ranjivosti standarda te su gotovo svi uređaji koji koriste WPA2 protokol podložni napadu.

KRACK sam po sebi ne omogućava otkrivanje lozinke bežične mreže nego napadaču omogućava pregled i dešifriranje podataka prenesenih napadnutom bežičnom vezom, te zbog toga izmjena lozinke bežične mreže ne može spriječiti ili ublažiti napad. Druga bitna napomena je ta da je KRACK još uvijek samo teorijski napad i nije zabilježen niti jedan slučaj zlouporabe. Razlog tome je činjenica da se za izvršenje napada, napadač mora nalaziti u području pokrivanja WLAN-a te je potrebna i žrtva koju bi napadač nagovorio na reinstalaciju već korištenog ključa. Nakon objave ovog napada, mnogi proizvođači opreme su s vremenom objavili razna sigurnosna ažuriranja i zakrpe koje umanjuju vjerojatnost KRACK-a.

3.5.4. Četvrta generacija metoda zaštite – nadolazeći WPA3

Nakon otkrivanja KRACK ranjivosti, Wi-Fi Alijansa je početkom 2018. objavila kako će do kraja godine omogućiti uporabu WPA3 protokola za bežičnu mrežu koji će zamijeniti WPA2 [20].

Prema prvim informacijama doznaje se kako će on uvesti nove mogućnosti za osobne i korporativne WLAN-ove, po [20] i [21]: robusnu zaštitu čak i onih korisnika koji odabiru

slabije lozinke od prosječne razine preporučene kompleksnosti. Olakšat će postupak konfiguracije zaštite za uređaje s ograničenim zaslonima ili bez njih. Primjeri su uređaji koji se koriste u internetu stvari (*Internet of things,* IoT).

Povećat će razinu sigurnosti korisnika koji se koriste otvorenim mrežama, pomoću individualizirane enkripcije podataka. Pretpostavlja se da je riječ o tek predloženoj oportunističkoj bežičnoj enkripciji (*Opportunistic Wireless Encryption*, OWE), koja pruža enkripciju podataka bez autentikacije. Koristit će 192 bitni ključ sukladan Komercijalnom nacionalnom sigurnosnom algoritmu (*Commercial National Security Algorithm*, CNSA).

3.5.5. Ostali oblici metoda zaštite bežičnih mreža

Virtualna privatna mreža (*Virtual private network*,VPN) može se koristiti kao jedan od oblika zaštite u bežičnim mrežama. Korištenjem VPN-a, korisnici osiguravaju podatke enkripcijom prilikom uporabe bežičnih mreža. Za potrebe osiguravanja toka podataka koriste se protokoli poput IPsec (*Internet Protocol Security Protocol), Transport Layer Security* (TLS) i zastarjeli *Secure Sockets Layer* (SSL) [1].

IPsec pruža napredne oblike zaštite kao što su algoritmi za bolju enkripciju i opsežniju autentifikaciju. SSL protokol je služio za siguran prijenos privatnih podataka putem mreže. Koristi asimetričnu kriptografiju kojom se razmjenjuju ključevi – javni ključ je poznat svima a privatni je poznat samo primatelju poruke. TLS je protokol kojim se osigurava privatnost u komunikaciji, tj. vodi računa o tome da poruke u komunikacijskom kanalu ne budu prisluškivane ili mijenjane od neke treće strane. Nasljednik je SSL protokola [25].

Kontrola pristupa mreži (*Network Access Control*, NAC) je vrsta autentikacijske tehnologije te sadrži pravila kojih se računala, koja se žele priključiti na mrežu, moraju pridržavati. Koristi se uz 802.1X standard kako bi se povećala razina zaštite u mreži. On kontrolira pristup mrežnim resursima na temelju korisničkog identiteta, stanju korisničkog uređaja i postavljenih sigurnosnih politika. Uz uporabu NAC-a, mrežni uređaji poput preklopnika, AP-a, usmjerivača i vatrozida, kontroliraju pristup po njegovim pravilima i odlukama.

Sustava za sprječavanje upada u bežičnoj mreži (*Wireless intrusion prevention system,* WIPS) služi identifikaciji i sprječavanju zlonamjernih upada ili napada u mreži te o tome obavještava osobe zadužene za sigurnost poput administratora sustava. Vatrozid ne može utjecati na pasivno prisluškivanje mreže, no WIPS može biti postavljen kako bi detektirao i sprječavao prijetnje i zlonamjerne aktivnosti u mreži. U kombinaciji s VPN-om, postaje snažna sigurnosna mjera koja aktivno nadzire mrežu s ciljem identifikacije anomalija. Ovime se dodatno osigurava povjerljivost podataka u mreži.

4. METODOLOGIJA VALIDACIJE SIGURNOSTI BEŽIČNE PRISTUPNE TOČKE

Validacija sigurnosti IK sustava, penetracijsko testiranje ili etičko hakiranje je oblik sigurnosne provjere učinkovitosti provedenih sigurnosnih mjera i mehanizama koje se koriste. Cilj ovog postupka je identificirati ranjivosti koje se nalaze u sustavu prije nego što iste budu otkrivene i iskorištene od napadača. Kako bi se dokazalo postojanje stvarne opasnosti u IK sustavu, osoba koja provodi testiranje pravno je odobrena za iskorištavanje pronađenih ranjivosti. Ovo poglavlje bavi se definicijom, razlozima provođenja, strategijama i metodologijama te objašnjava različite oblike testiranja uz faze kroz koje se prolazi u postupku.

4.1. Definicija validacije sigurnosti

Validacija sigurnosti ili penetracijsko testiranje je tehnika procjene sigurnosti IK sustava ili njegove mreže, a temelji se na odobrenoj simulaciji stvarnog napada. Prilikom testiranja, ovlašteni ispitivač izlaže ciljani IK sustav različitim vrstama napada a oni su slični onima koje bi koristio i stvarni napadač na takav sustav. Cilj mu je uočiti bilo kakvu ranjivost koju je moguće iskoristiti za ostvarenje neovlaštenog pristupa i ugrožavanje sustava [29].

Ovakav način testiranja daje rezultate i pronalazi mane, međutim često se precjenjuje njegov značaj. Uspješnost prilikom prolaska sustava na testu ne dokazuje da je sustav zaista potpuno siguran. Vrijeme provođenja pojedinog testa varira. Penetracijski test je pokušaj narušavanja sigurnosti IK sustava te nije potpuna potvrda da on siguran. To je samo pogled na stanje sigurnosti sustava u trenutku provođenja testa [8].

Penetracijski test također može imati ozbiljnih posljedica za mrežu u kojoj se provodi te uzrokovati zagušenje mreže ili rušenje IK sustava. U slučaju lošeg ili neoprezno provedenog testiranja, IK sustav može biti izložen gubitku podataka, kvaru u komunikaciji ili drugim greškama koje direktno utječu na njegov rad i načela sigurnosti [29].

On završava detaljnim opisom pronađenih i iskorištenih ranjivosti te objašnjenjem kako je ranjivost bila iskorištena. Poželjno je da ovaj dio sadrži preporuke i smjernice za ispravljanje problema otkrivenih tijekom testiranja. Ovaj proces služi kao pomoć u zaštiti IK sustava od potencijalnih napada. Glavni zadatak testiranja je otkrivanje sigurnosnih propusta u sustavu uporabom istih programskih alata, metoda i načinom razmišljanja kao napadač. Općeniti cilj testiranja je identifikacija, dokazivanje i uklanjanje ranjivosti prije nego iste budu iskorištene od strane zlonamjernih korisnika IK sustava [14].

4.2. Razlozi provođenja validacije sigurnosti

Postupak penetracijskog testiranja unutar organizacije odnosno njenog IK sustava, provodi se zbog sljedećih razloga, [8]:

- kako bi se testirala i ocijenila učinkovitost implementiranih metoda zaštite i sigurnosnih kontrola

- kako bi se ustanovile ranjivosti kojima je sustav podložan
- za prikupljanje korisnih informacija s ciljem provjere pridržavanja određenih regulatornih okvira
- za smanjenje troškova sigurnosnih procjena zbog posjedovanja jasnih i realnih dokaza o mogućnostima organizacije
- kao pomoć prilikom određivanja prioriteta u primjeni zakrpi za prijavljene ili poznate ranjivosti
- za određivanje trenutnog stanja rizika u kojem se nalazi IK sustav organizacije
- za potrebe validacije učinkovitosti sigurnosnih mrežnih uređaja poput vatrozida, usmjerivača, preklopnika i *web* poslužitelja
- za pružanje jasnog pristupa u pripremi koraka koji se poduzimaju s ciljem sprječavanja napada ili iskorištavanja IK sustava u budućnosti
- za utvrđivanje potrebne nadogradnje ili promjene postojećeg softvera, hardvera ili dijela mrežne infrastrukture

Glavni razlog provođenja validacije sigurnosti je identifikacija i ispravljanje svih sigurnosnih propusta sustava prije uzrokovanja štete. Uz to postoje i drugi [29]:

Otkrivanje propusta prije napadača – napadači koriste veliki broj automatiziranih alata za traženje propusta u IK sustavu ili mreži koje mogu iskoristiti te neovlašteno pristupiti sustavu. Mali broj njih koristi napredne tehnike odnosno još javno nepoznate ranjivosti (*zero day exploit*), dok se većina koristi dobro poznatim i predvidivim načinima napada. Mrežni administratori koriste penetracijske testove kako bi dobili jasnu sliku ranjivosti u njihovoj mreži. Cilj ovakvog penetracijskog testa je pronaći ranjivosti sustava kako bi se takvi mogli ispraviti prije nego ih otkrije napadač.

Izvještavanje menadžmenta o problemima – rezultati penetracijskog testa pomažu u opravdanju izdvajanja sredstava potrebnih za rješavanje sigurnosnih nedostataka u sustavu. Informatičko osoblje organizacije obično je svjesno slabosti u sigurnosti IK sustava, no problem je u to uvjeriti menadžment kako bi odobrio obavljanje potrebnih promjena. On ima više poštovanja i ozbiljnije prihvaća mišljenja vanjske ekspertne grupe za sigurnost (*outside security expert*). Koristeći neutralnu stranu koja ne posjeduje unutarnje znanje, penetracijski tim može identificirati iste ranjivosti uočene od unutrašnjeg tima te uvjeriti menadžment kako bi ranjivosti trebale biti uklonjene. Krajnja odgovornost za sigurnost informacijske tehnologije stoji na menadžmentu jer oni odlučuju koja je prihvatljiva razina rizika za organizaciju.

Sigurnosna obuka za informatičko osoblje – penetracijski testovi informatičkom osoblju pružaju priliku da prepozna i odgovori na razne oblike mrežnih napada. Ako penetracijski ispitivač uspješno kompromitira sustav bez ičijeg znanja, to je indikator neadekvatnog pristupa obuci osoblja zaduženog za sigurnost. Osoblje zaduženo za testiranje, praćenje i rješavanje sigurnosnih incidenata, na ovaj način može pokazati svoje sposobnosti uočavanja situacija u IK sustavu te pokazati efektivnost odgovora na otkriveni napad. Kada osoblje za sigurnost ne uspije identificirati neprijateljsku aktivnost, rezultati penetracijskog testiranja mogu biti korisni za usavršavanje njihovih vještina na odaziv i uklanjanje neprimjerenih aktivnosti u sustavu.

Testiranje novih tehnologija – idealno vrijeme za testiranje nove tehnologije je upravo prije puštanja u pogon. Izvođenjem penetracijskog testa na novim tehnologijama, aplikacijama i njihovoj okolini prije javne aktivnosti često znači uštedu vremena i novca. Razlog tome je činjenica da je jednostavnije testirati i modificirati novu tehnologiju o kojoj nitko ne ovisi. Primjeri su testiranje novog *web* poslužitelja ili nove bežične infrastrukture.

4.3. Metodologije i strategije validacije sigurnosti

Kako bi se zadovoljile potrebe penetracijskog testiranja IK sustava, razvijene su mnoge metodologije koji definiraju proces. Primjenom razvijenih radnih okvira moguće je strateški provesti penetracijsko testiranje, neovisno o veličini i kompleksnosti promatranog IK sustava.

Osnovni cilj formalizacije procesa penetracijskog testiranja je mogućnost izvršavanja raznovrsnih testova korak-po-korak, kako bi se trenutno stanje sigurnosti IK sustava što točnije procijenilo [14] i [8].

Najpoznatije razvijene metodologije penetracijskog testiranja su:

- OSSTM – *Open Source Security Testing Methodology*
- ISACA – *Information Systems Audit and Control Association*
- ISSAF – *Information System Assessment Framework*
- OWASP – *Open Web Application Security Testing Guide*
- WASC – *Web Application Security Consortium Threat Classification*
- PTES – *Penetration Test Execution Standard*

Prilikom izrade rada najviše su se pratile smjernice PTES-a iz razloga njegove slobodne dostupnosti, iscrpnosti i detalja prilikom testiranja. Uz navedeno isti pruža pomoć i smjernice za testiranja različitih oblika mreža među kojima su primjeri i za WLAN standard.

Validacija sigurnosti IK sustava pojavljuje se u različitim oblicima ovisno o elementu sustava koji se testira. Strategije koje se koriste prilikom provođenja testiranja su po [8], sljedeće:

- Validacija sigurnosti javnog dijela IK sustava (*External penetration testing*) – uglavnom se provodi nad poslužiteljima, softveru jezgre i drugim ključnim dijelovima infrastrukture sustava. Strategija korištena prilikom validacije sigurnosti korporacija.
- Validacija sigurnosti unutarnjeg dijela IK sustava (*internal penetration testing*) – ova strategija omogućuje jasan uvid u sigurnosno stanje IK sustava organizacije.
- Validacija sigurnosti *web* aplikacija (*Application security assessment*) – aplikacije danas predstavljaju najranjiviji i najizloženiji oblik softverskog elementa IK sustava.
- Validacija sigurnosti računalne mreže (*Network security assessment*) – identificira rizike i ranjivosti koji mogu ugroziti mrežu i pripadajuće sigurnosne politike. Pruža informacije potrebne za provođenje sigurnosnih odluka u mreži

- Validacija sigurnosti bežičnog/udaljenog pristupa (*Wireless/remote-access security assessment*) – posvećeno je istraživanju sigurnosnih rizika vezanih za bežične uređaje u mreži IK sustava. Većina validacija obavlja se za potrebe 802.11 standarda.
- Validacija sigurnosti telefonske linije (*Telephony security assessment*) – bavi se problemima u području glasovnih tehnologija. Primjeri su iskorištavanje privatne telefonske centrale (*Private Branch Exchange*, PBX) kako bi se uspostavili posebno tarifirani pozivi s ciljem izazivanja financijskog troška i drugi.
- Procjena pomoću socijalnog inženjeringa (*Social-engineering assessment*) – ovom tehnikom napada se ljudski element IK sustava s ciljem dolaska do informacija koje bi mogle naštetiti sustavu. Tehnike napada su prisluškivanje, kopanje po kontejnerima otpada u potrazi za odbačenim spisima organizacije, te napadi preko *e-maila* naziva *phishing* ili njegov napredniji oblik *spear phishing*.

U ovom radu bit će provedeno testiranje koje je spoj strategija validacije sigurnosti računalne mreže i sigurnosti bežičnog/udaljenog pristupa.

4.4. Vrste sigurnosnih procjena u IK sustavima

Ne postoji samo jedan oblik validacije sigurnosti nego se oni dijele na njih nekoliko, ovisno o složenosti procjene koja se radi. Tipovi sigurnosnih procjena (*security assessment*) po [30] su: procjena ranjivosti, tradicionalno penetracijsko testiranje i penetracijski test na temelju usklađenosti.

4.4.1. Procjena ranjivosti

Procjena ranjivosti (*Vulnerability assessment*) je postupak zapisivanja otkrivenih ranjivosti unutar ciljanog okruženja. Koncept ciljanog okruženja vrlo je bitan, jer je prilikom procjene važno ostati unutar određenog obuhvata ciljane mreže i zadataka koji se moraju izvršiti. U slučaju prekoračenja obuhvata procjene, može doći do smetnji usluga na mreži, gubitka povjerenja klijenta ili pak tužbi protiv osobe ili firme koja se bavi procjenom [30].

Drugi naziv je skeniranje ranjivosti (*Vulnerability Scanning*) zbog razloga korištenja automatiziranih softverskih alata koji pretražuju IK sustav s ciljem identifikacija potencijalnih ranjivosti. To je planska i metodološka procjena izloženosti imovine poduzeća zlonamjernim napadačima, prirodnim nepogodama i entitetima koji potencijalno mogu uzrokovati štetu. Cilj je identificirati onu imovinu koja mora biti zaštićena, vrste prijetnji kojima je podložna, procijeniti trenutne razine sigurnosti te procjenu štete od pojedinih izvora prijetnji [1].

Netko se može pitati koja je razlika između penetracijskog testiranja i procjene ranjivosti. Oba postupka daju procjenu mogućih napada na sustav. Ipak, pretraživanje ranjivosti, procjenu stvara na temelju automatiziranog procesa, te ga se smatra uvodnim korakom penetracijsko testiranje koje potvrđuje ili opovrgava ranjivosti detektirane automatskim procesom. Za razliku od pretraživanja ranjivosti, penetracijsko testiranje daje skup otkrivenih i iskorištenih ranjivosti koje se nalaze u sustavu [29].

Zbog svoje relativne jednostavnosti, ovakva testiranja se provode često u razvijenim okruženjima kao dio demonstracije dubinskog ispitivanja (*due diligence*). U većini slučajeva koriste se automatski alati tzv. skeneri ranjivosti (*Vulnerability Scanner*). Pomoću njih je moguće otkriti dostupne uređaje u ciljanom okruženju te identificirati usluge i informacije poput: softvera poslužitelja, verzije, platforme i sl. Te informacije se potom provjeravaju s poznatim potpisima (*signature*) potencijalnih problema ili ranjivosti [30].

Potpisi su izrađeni od kombinacije podatkovnih točaka (*data points*) koje su namijenjene prikazivanju problema. Podatkovne točke su skupovi velikog broja informacija o IK sustavu, određenom dijelu ili uređaju koji se nalazi u njemu a pomoću njih je moguće saznati više o potencijalnim ranjivostima koje prijete IK sustavu. Više podatkovnih točaka se koristi sa svrhom što točnije identifikacije ranjivosti. Među njima su [30]:

- Verzija operativnog sustava - nije neuobičajeno da softver ima ranjivost na jednom OS a na drugom ne. Zbog toga, skeneri pokušavaju što točnije odrediti koju verziju OS-a koristi računalo na kojoj se pokreće određena aplikacija
- Razina zakrpe (*Patch Level*) – dosta često, dolazi do izdavanja zakrpi za OS koje ne mijenjaju informacije o verziji ali umanjuju ranjivosti ili ih potpuno uklanjaju
- Arhitektura procesora – mnoge aplikacije su dostupne za više vrsti procesorskih arhitektura poput Intel x86, Intel x64, različite verzije *ARM*-ova, *UltraSPARC* i sl. U nekim slučajevima, ranjivosti postoje samo na određenoj arhitekturi stoga su te informacije bitne za utvrđivanje ispravnog potpisa.
- Verzija softvera – verzija ciljanog softvera je jedna od osnovnih stvari koje se moraju saznati kako bi se identificirala ranjivost

Ovi podaci se koriste za izradu potpisa kao dio procjene ranjivosti. Što više podatkovnih točaka se podudara, to će potpis biti točniji. Kada se govori o podudaranju potpisa, postoji nekoliko različitih potencijalnih rezultata, po [30]:

- Istinski pozitivan (*True Positive*) - potpis se podudara i zahvaća stvarnu ranjivost. Ovakvi rezultati su oni koje treba slijediti i ispraviti iz jer su to stvari koje zlonamjerni korisnici mogu iskoristiti za nanošenje štete sustavu
- Lažno pozitivni (*False Positive*) – potpisi se podudaraju, međutim otkriveni problem nije stvarna ranjivost. U procjeni, ovakvi rezultati su često smatrani smetnjom te mogu biti vrlo frustrirajući. Prilikom provođenja procjene, velika greška je odbaciti istinski pozitivan potpis kao negativno pozitivan bez dodatne provjere
- Istinski negativan (*True Negative*) – potpis se ne podudara te ne postoji ranjivost. Ovo je idealan slučaj koji potvrđuje da ne postoji ranjivost na ciljanom sustavu.
- Lažno negativan (*False Negative*) – potpis se ne podudara ali postoji ranjivost. Iako je lažno pozitivan potpis loša stvar, lažno negativan potpis je puno gori od toga. U tom slučaju, problem postoji ali ga skener nije detektirao te stoga nema indikacije da postoji.

Točnost potpisa važna je za dobivanje točnih rezultata. Što je više podataka skupljeno, veća je šansa za točniji rezultat dobiven alatom za automatsko skeniranje potpisa.

Kod autenticiranog skeniranja, alat za skeniranje koristi korisničke podatke s kojima se autenticira na računalu. Ovaj postupak omogućuje bolji uvid u ciljani IK sustav. Na primjer,

obično skeniranje pruža informacije o sustavu temeljem usluga koje se odvijaju na njemu i funkcionalnosti koje pružaju. Iako je ovim putem moguće doći do mnogo informacija, ovakav način skeniranja ne može se mjeriti s količinom i značajem podataka koji se prikupe autentikacijom u sustav. Nakon nje se s razumijevanjem može pregledati instaliran softver, primijenjene zakrpe, pokrenuti procesi i sl. Ovakav opseg podataka je koristan za otkrivanje ranjivosti koje inače ne bi bile identificirane [30].

Dobro provedena procjena ranjivosti daje uvid u potencijalne probleme u organizaciji te pruža mjere i načine kako bi se isti ispravili tijekom vremena. Ovo je ublažena verzija procjene, koju mnoge organizacije provode kako bi se izbjegli potencijalni problemi u vrijeme kad su resursi, poput usluga i širine propusnog pojasa, najpotrebniji.

Budući da se automatizirani alati koriste bazama podataka potpisa za detekciju ranjivosti, bilo kakvo odstupanje od poznatog potpisa iz baze, može izmijeniti rezultat skeniranja ili valjanost uočene ranjivosti. Lažni pozitivni potpis označuje ranjivost koja ne postoji, dok lažni negativni potpis ne uočava stvarnu ranjivost koja nije prijavljena u rezultatu [30].

Poseban problem javlja se u činjenici ne postojanja standardiziranog načina za prikupljanje, analizu i prijavu ranjivosti. Ako se procjena radi s nekoliko alata, od različitih proizvođača, za svaki je potrebno proučiti veliki broj informacija tj. podatkovnih točaka koje je potom potrebno interpretirati kako bi se utvrdilo postojanje ranjivosti. Takav način provođenja procesa utvrđivanja ranjivosti često je naporan i dugotrajan posao [1].

Zbog toga se često kaže, da je skener dobar onoliko koliko je dobra njegova baza potpisa. Iz tog razloga mnogo proizvođača opreme, mora izraditi dva kompleta potpisa [30]:

- jedan koji je besplatan i jednostavan te zadovoljava potrebe korisnika mreže običnog kućanstva
- drugi koji je izrazito kompleksan skup potpisa te se prodaje korporacijama.

Ispravno napisano izvješće procjene ranjivosti može poslužiti kao temelj za druge oblike procjena poput penetracijskog testa na temelju usklađenosti.

4.4.2. Penetracijski test na temelju usklađenosti

Sljedeća vrsta procjene je penetracijski test na temelju usklađenosti (*Compliance Penetration Test*) [30]. Iako postoji mnogo okvira za usklađenost prema različitim industrijskim granama, najčešće se koristi Standard za sigurnost podataka, industrije platnih kartica (*Payment Card Industry Data Security Standard*, PCI DSS) [31].

To je regulatorni okvir kojim proizvođači platnih kartica, obvezuju trgovce, koji koriste mogućnost naplate putem kartica. Postoje i drugi standardi poput, [30]:

- Vodiča za tehničku implementaciju sigurnosti, Agencije za obrambene informacijske sustave
  (*Defense Information Systems Agency Security Technical Implementation Guides*, DI SA STIG),

- Federalni program za upravljanje rizikom i autorizacijom (*Federal Risk and Authorization Management Program*, FedRAMP),
- Federalni upravljački akt za informacijsku sigurnost (*Federal Information Security Management Act*, FISMA) te drugi.

Bilo da su obavezne ili proizvoljne, ovakve vrste procjene se kolektivno zovu penetracijski testovi na temelju usklađenosti, procjena ili provjera usklađenosti.

Testiranje započinje provjerom ranjivosti. U slučaju provjere po [30], ispravno odrađena procjena ranjivosti udovoljava osnovnim zahtjevima poput:

- " 2. Ne koristiti zadane korisničke lozinke koje je postavio proizvođač opreme",
- "11. Redovito testirati sigurnost sustava i procesa".

Neki zahtjevi, poput "9. Ograničiti fizički pristup podacima korisnika kartice" i "12. Provoditi politiku informacijske sigurnosti koja se odnosi na cijelo osoblje", ne idu na korist procjenama ranjivosti s automatiziranim alatima te zahtijevaju dodatnu kreativnost i testiranja.

Svi trgovci koji koriste kartice, moraju zadovoljavati propisane PCI DSS zahtjeve za WLAN. U zahtjevima je obavezna uporaba vatrozida, te detaljan pregled mreže kako bi se isključilo postojanje zlonamjernih pristupnih točaka (*rogue wireless access point*), [31].

Uz navedeno, od IK sustava koji koriste WLAN uređaje u mreži, očekuje se dodatna pažnja prilikom uporabe i implementacije u sustav, poput [31]:

- Fizička sigurnost WLAN uređaja
- Promjena tvornički postavljenih lozinki i postavki uređaja koji se nalaze u WLAN mreži
- Praćenje elektroničkih zapisa tj. izvještaja o stanju sustava (*Logging*, *Event log*) bežičnog pristupa mreži te uporaba sustava zaštite od neovlaštenog upada (*Intrusion Prevention System, IPS*)
- Snažnu autentikaciju i enkripciju koja se koristi u mreži
- Uporabu snažne kriptografije i sigurnosnih protokola
- Razvoj i pridržavanje sigurnosne politike o uporabi ovakve mreže

4.4.3. Tradicionalno penetracijsko testiranje

Pojam tradicionalnog penetracijskog testiranja postaje sve teže definirati, zbog mnogih različitih definicija koje su u uporabi. Dio ove zabune je zbog činjenice da se izraz "penetracijsko testiranje" danas više koristi za penetracijski test na temelju usklađenosti (a ponekad čak i za procjenu ranjivosti) [30].

Za razliku od dosad razmatranih vrsti procjena, penetracijski testovi ne počinju uvijek definiranjem obuhvata, nego s ciljevima poput:

- "simulacije događaja koji bi se dogodio ukoliko (unutarnji) korisnik bude kompromitiran" ili

- "identificirati što će se dogoditi ako organizacija bude izložena napadu vanjskog zlonamjernog korisnika"

Za razliku od procjene ranjivosti, u penetracijskom testiranju dolazi do stvarnog iskorištavanja ranjivosti koje su pronađene u sustavu. Osim uz uporabu automatskih skenera ranjivosti, u ovom obliku procjene veliku važnost imaju znanje, iskustva, umijeća i lukavost osobe koja provodi testiranje. Uobičajena je praksa da ovakav test provodi stručno licencirana osoba, koja nije nužno zaposlenik poduzeća koje testira sustav ali posjeduje pravno odobrenje od uprave za provođenje ovakvog testiranja [1].

Umjesto oslanjanja samo na snažne skenere ranjivosti, potrebno je provjeriti dobivene rezultate testiranjem, kako bi se uklonili lažni pozitivni potpisi i otkrile prave ali skrivene ranjivosti IK sustava. Ovo često uključuje iskorištavanje otkrivenih ranjivosti, istraživanje razine pristupa koje iskorištavanje ranjivosti nudi te ponovnim napadom na metu uz pomoću veće razine pristupa [30].

Postupak zahtijeva kritičan osvrt, ručno istraživanje, kreativnosti te razmišljanje izvan okvira kako bi se otkrile potencijalne ranjivosti. Nakon završetka, ovaj proces je potrebno ponoviti nekoliko puta kako bi se posao napravio detaljno i kompletno.

4.5. Faze validacije sigurnosti

Kao i svaki postupak, validacija sigurnosti odvija se po nekoliko faza. Razni izvori sadrže različiti broj (od četiri do sedam) koraka ili faza. Razlog tome je postojanje nekoliko vrsti metodologija po kojoj autori pišu o penetracijskom testiranju. Uz to, nije neuobičajeno da postoje male razlike u nazivima te činjenice da se neke faze jednog autora, smatraju podfazama u drugim literaturama. Kako bi se objasnile sve faze koje se pojavljuju u ovom postupku, odlučeno je da su to sljedeći koraci, po [14], [29], [30], [32] i [33]:

1. Faza pripreme testiranja (*Pre-engagement Interactions*)

- Svrha ove faze je određivanje vremenskog perioda, opsega i uvjeta penetracijskog testa,
- ključno je oblikovati sve ciljeve postupka,
- u ovoj fazi, klijent koji zahtjeva testiranje, upućen je u ishode testiranja te se bilježe razlozi zahtjeva testiranja IK sustava

2. Prikupljanje informacija (*Information Gathering*)

- Neka od imena faze su i prepoznavanje ili praćenje tragova (*Reconnaissance*, *footprinting*),
- u ovoj fazi, potrebno je doznati što je više moguće o ciljanoj okolini IK sustava,
- aktivnosti koje se obavljaju su ne invazivne te se čine kao standardna korisnička aktivnost,
- predstavlja temelj za ostatak validacije te treba biti što točnije izvedena,

- primjeri informacija koji se mogu prikupiti u ovoj fazi: podaci o zaposlenicima, telefonski brojevi, opseg IP adresa, informacije o postrojenju i informacije o poslovanju,
- konačni rezultat bi trebao biti grubi profil mete napada ali opet dovoljnim za provedbu faze koja slijedi,

3. Otkrivanje ranjivosti (*Vulnerability Discovery*)

- često se naziva i "aktivno prikupljanje informacija" (*Active Information Gathering*), skeniranje mreže (*network scanning*) ili nabrajanje (*Enumeration*),
- prilikom provedbe se ne izvršava napad ali se pokreće ne standardna korisnička aktivnost s ciljem identificiranja potencijalnih ranjivosti u ciljanom okruženju,
- Skeniranjem mreže lociraju se aktivna računala su napadnuta u sljedećoj fazi, za to se koriste: *ping, ping sweeps,* skeneri *portova, tracert* i ostali*,*
- ovo je faza u kojoj se najčešće događa skeniranje ranjivosti raznim automatiziranim alatima,
- Podaci prikupljeni tijekom faze uključuju: korisnička imena, lozinke, informacije o uređajima, planovi ili mrežni dijagrami, informacije o protokolima, podaci o poslužiteljima i informacije o uslugama

4. Iskorištavanje ranjivosti (*Exploitation*)

- Proboj ili napad na IK sustav, poznat i kao postupak hakiranja,
- U ovoj faza dolazi do iskorištavanja prethodno otkrivenih ranjivosti kako bi se dobila polazna točka za napad,
- Kompleksna faza koja sadrži različite pristupe poput probijanja lozinki, povećanja razina pristupa u mreži, uporabe različitih aplikacija

5. Pivotiranje i izvlačenje podataka iz IK sustava (*Pivoting and Exfiltration*)

- nakon ostvarivanja polazne točke, potrebno je ostvariti daljnje korake poput povećanja razine korisničkih privilegija koje napadač ima u IK sustavu, kako bi se ostvarili predviđeni ciljevi napada,
- pivotiranje u ostale dijelove sustava koji su do tada bili nedostupni, s ciljem izvlačenja povjerljivih informacija

6. Izvještavanje (*Reporting*)

- nakon završetka aktivnog dijela procjene, potrebno je dokumentirati i prijaviti sve provedene aktivnosti,
- ova faza nije tehnička kao prethodne no vrlo je važno osigurati da klijent dobije punu vrijednost obavljenog posla.

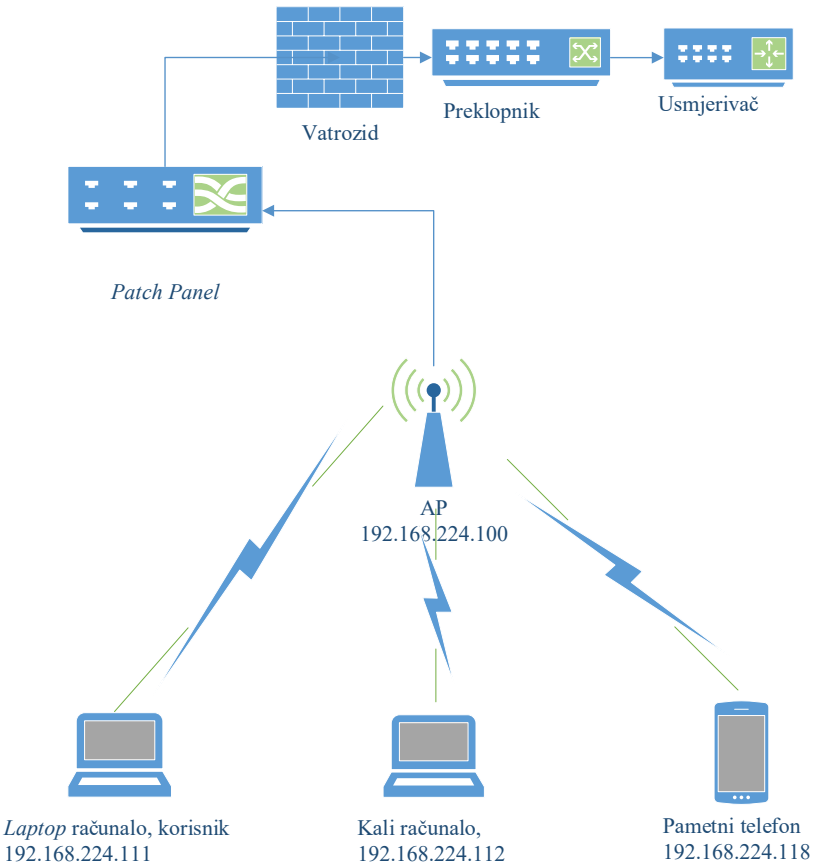
5. PROVEDBA VALIDACIJE SIGURNOSTI U LABORATORIJSKOM OKRUŽENJU

Postupak validacije sigurnosti provodi se koracima navedenim u prošlom poglavlju. U ovom poglavlju bit će opisane dvije iteracije procesa. U prvoj iteraciji objasnite će se postupak prikupljanja informacija s automatiziranim alatom *Maltego* i mrežnog skenera *Nmap* koji se također može koristiti u te svrhe. U sklopu testa izvesti će se MITM napad na terminalni uređaj povezan na AP laboratorija.

Druga iteracija opisuje mogućnosti koje napadač ima nakon povezivanja tj. ostvarivanja pristupa na nezaštićeni AP. Istražit će se put kojim se terminalni uređaj, u WLAN mreži laboratorija, spaja na internet stranicu Fakulteta prometnih znanonsti www.fpz.hr. Identificirat će se put kojim paketi prolaze kroz mrežu tj. čvorove na ruti od terminala do *web* poslužitelja fakulteta.

5.1. Validacija pristupne točke i povezanih uređaja

Shema laboratorija za postupak testa prikazana je slikom 2. Laboratorijsko okruženje se sastoji od usmjerivača, preklopnika, vatrozida, *patch* panela, AP-a i povezanih terminalnih uređaja na njoj.



Slika 2. Izgled laboratorijskog okruženja

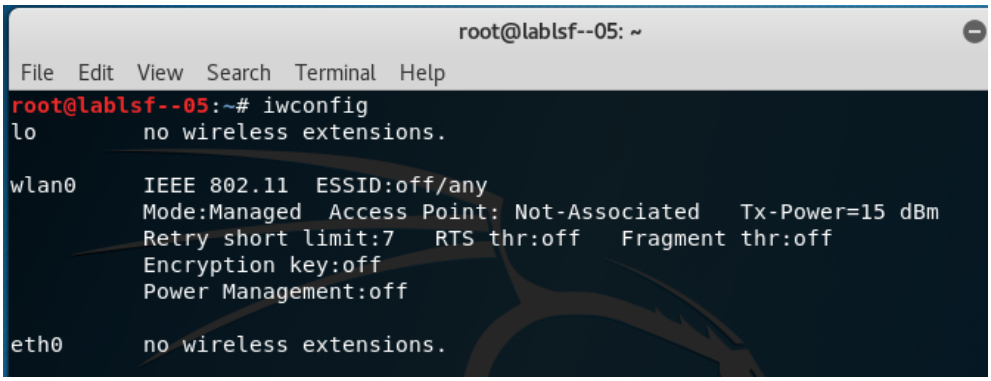
Usmjerivač je izlazna točka iz Laboratorija, na njega se spajaju preklopnik na kojem je spojen vatrozid te AP. Terminalni uređaji spojeni na AP su *laptop* na koji je instaliran Kali Linux, korisnikovo računalo koristi *Windows7 Pro* i pametni telefon *Samsung* koji radi na *Linux* OS *Android* v.7, *Nougat*.

5.1.1. Faza pripreme testiranja

Ovom fazom određen je vremenski period izvođenja validacije i opsega (laboratorij fakulteta). Ciljevi su istražiti oblike informacija kojima je moguće pristupiti nakon povezivanja na pristupu točku *FreeWiFi* u laboratoriju. Naglasak je na tome da promatrani AP ne posjeduje nikakav oblik sigurnosne zaštite (WPA ili WPA2) nego je otvoren.

Postupak povezivanja na AP, pomoću uporabe naredbene linije ili retka (*Command-Line Interface/Interpreter*, CLI) je sljedeći:

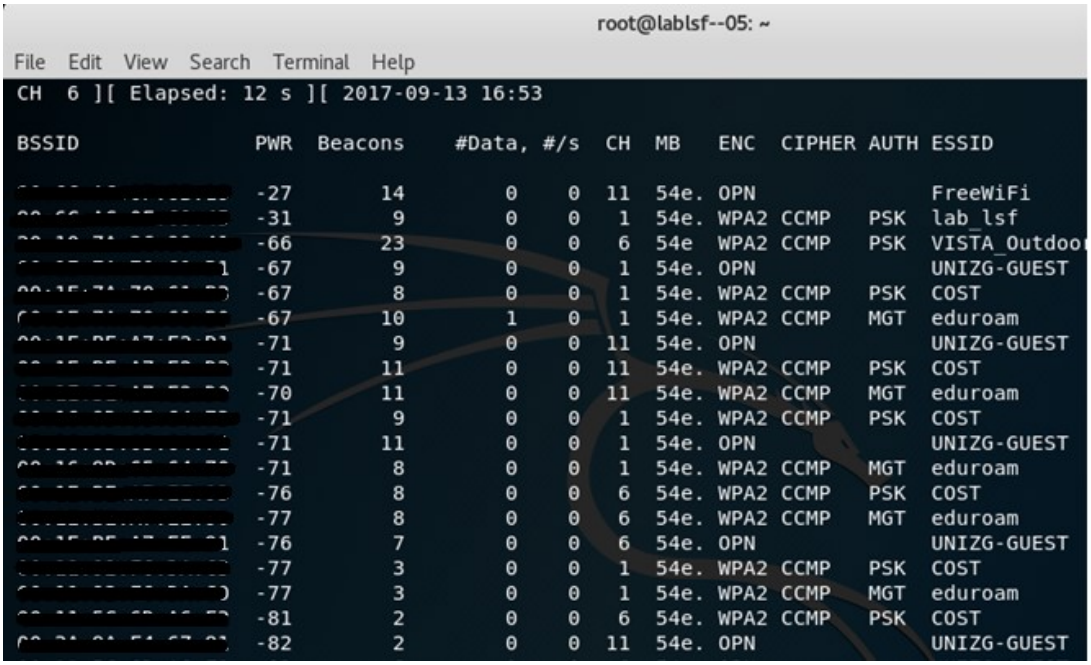
Potrebno provjeriti konfiguraciju računala na kojem se koristi posebna vrsta OS-a, posvećena penetracijskom testiranju naziva Kali Linux. Konfiguracija hardvera dobiva se naredbom *Iwconfig,* a rezultati su prikazani slikom 3.



Slika 3. *Iwconfig*

Ona prikazuje dostupna mrežna sučelja korištenog računala. Naredba vraća parametre poput standarda koji podržava NIC korištenog računala, trenutni način rada kartice (oblici su *managed* - korišten za spajanje na AP ili *monitor* – koji se koristi za osluškivanje svih paketa tj. AP *becona* koji se odašilju u dometu). Također prikazuje ime povezanog AP-a, snagu odašiljanja signala i drugo.

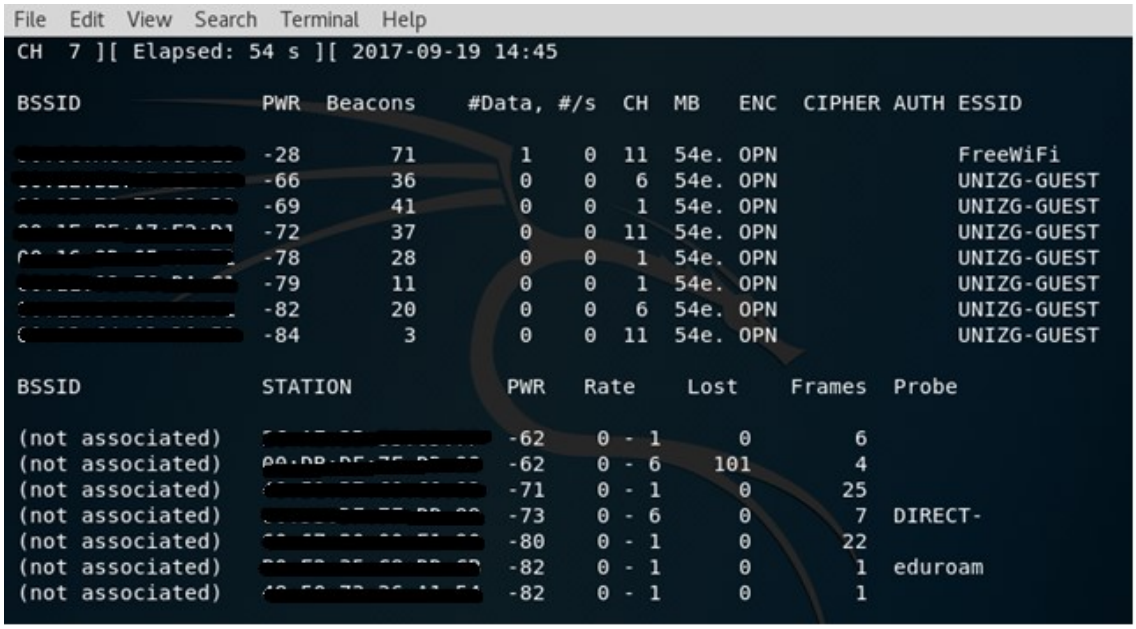
Za otkrivanje dostupnih AP-ova, u Kali-u se koristi skup alata pod nazivom „*aircrack-ng "*te njegove pod alate poput „*airodump-ng "*. Za sljedeći korak, potrebno je prebaciti način rada kartice iz *managed* u *monitor* korištenjem *airmon-ng* alata (rezultat je novi naziv *wlan0mon*). Za identifikaciju pristupne točke koristi se naredba *airodump-ng*, slika 4. Pomoću nje, hvataju se okviri 802.11. standarda a alat to prikazuje kao zapis svih AP-ova koji emitiraju signal u dosegu korištene mrežne kartice.



Slika 4. Rezultati airodump-ng naredbe

Naredbom se dolazi do mnogih informacija poput: MAC adrese AP-a (BSSID), njegove snage (PWR), kanala na kojem radi (CH), brzine pristupa (MB), korištenoj enkripciji (ENC), šifratu (CIPHER) i vrsti autentikacije (AUTH) te naziva točke (ESSID).

Detaljnijom naredbom u *airdump-ng,* moguće je izdvojiti AP koji nemaju nikakvu zaštitu. Dodavanjem parametara *–encript OPN,* dobiva se puno jednostavniji rezultat, slika 5, gdje se uz AP vide i klijenti (*station*) spojeni na mrežu.



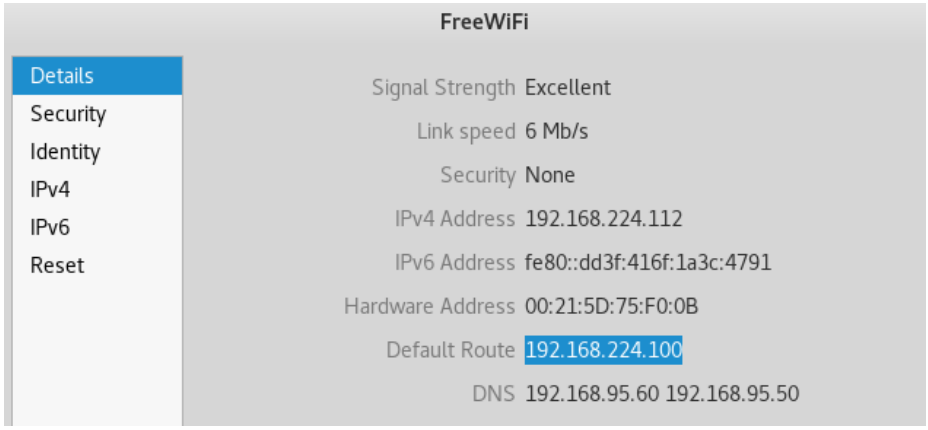
Slika 5. Filtrirani popis AP

Ciljani AP koji je odobren za potrebe validacije sigurnosti ima naziv "*FreeWiFi*". Pokušaj provedbe bilo koje od faza testiranja na drugom AP-u vjerojatno bi završio kaznenim progonom od strane Sveučilišta u Zagrebu.

Zbog toga što je AP otvoren, odnosno ne provode se sve moguće mjere zaštite pristupa, povezivanje na istu spada pod fazu pripreme testiranja. U stvarnim uvjetima testiranje bi započeo sličnim koracima, no cilj prve iteracije (u testiranju IK sustava, faze se provode mnogo puta s ciljem što detaljnijeg ispitivanja sustava), bio bi probijanje jedne od vrste sigurnosnih protokola kojima se ojačava zaštita bežičnog AP-a. Postupak opisan u radu preskače taj korak te je moguće pristupiti mreži i započeti s pokušajem ugrožavanja IK sustava tj. WLAN mreže fakulteta.

5.1.2. Prikupljanje informacija

Cilj ovog koraka je prikupljanje informacija o okolini u kojoj se test provodi. Najjednostavniji način za dobivanje prvih informacija o mreži fakulteta, je čitanjem postavki mreže na korištenom računalu, prozor izbornika je vidljiv na slici 6.



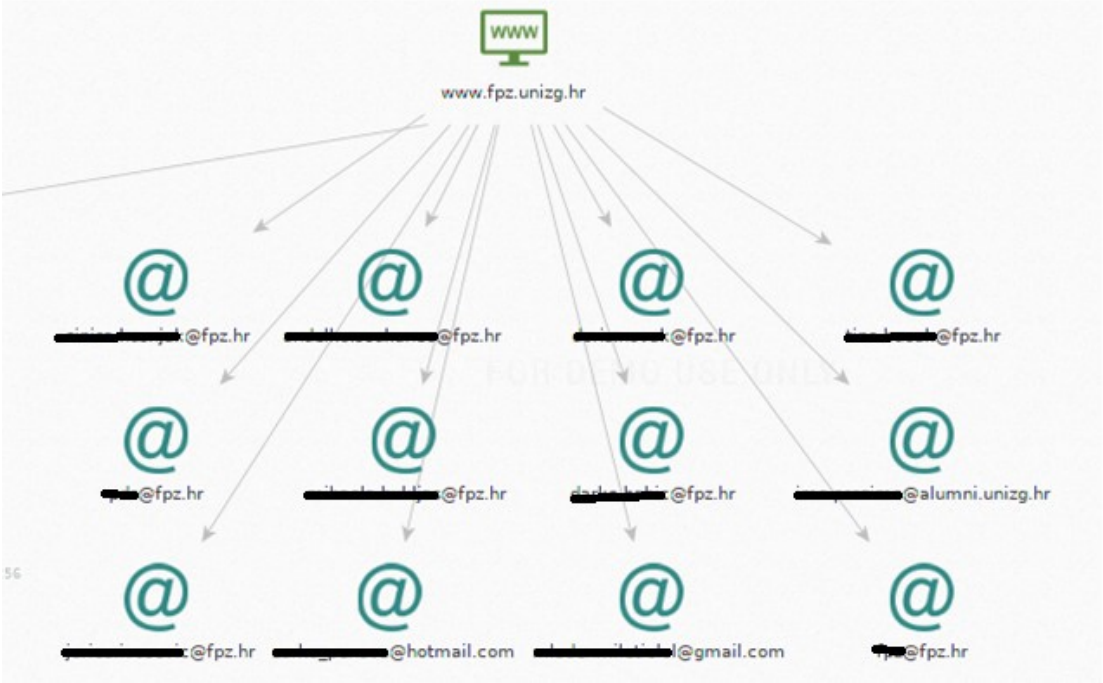
Slika 6. Izbornik postavki mreže

U njemu je moguće vidjeti brzinu pristupa, verzije IPv4 i IPv6 adresa koje *Kali* ima u mreži. Uz navedeno, mogu se iščitati IP adrese dodijeljene rute i sustava imenovanja domena (*Domain Name System*, DNS). Ovo je korisno radi daljnjeg istraživanja mreže te zbog razloga što je DNS prepun korisnih informacija o mreži IK sustava u kojem se nalazi.

Kako bi se prikupile detaljnije informacije o sustavu koriste se mnogi alati dostupni iz *Kali* operativnog sustava. Za potrebe ovog rada, u sljedećim potpoglavljima opisano je korištenje alata *Maltego* i *Nmap* za potrebe ove faze testiranja.

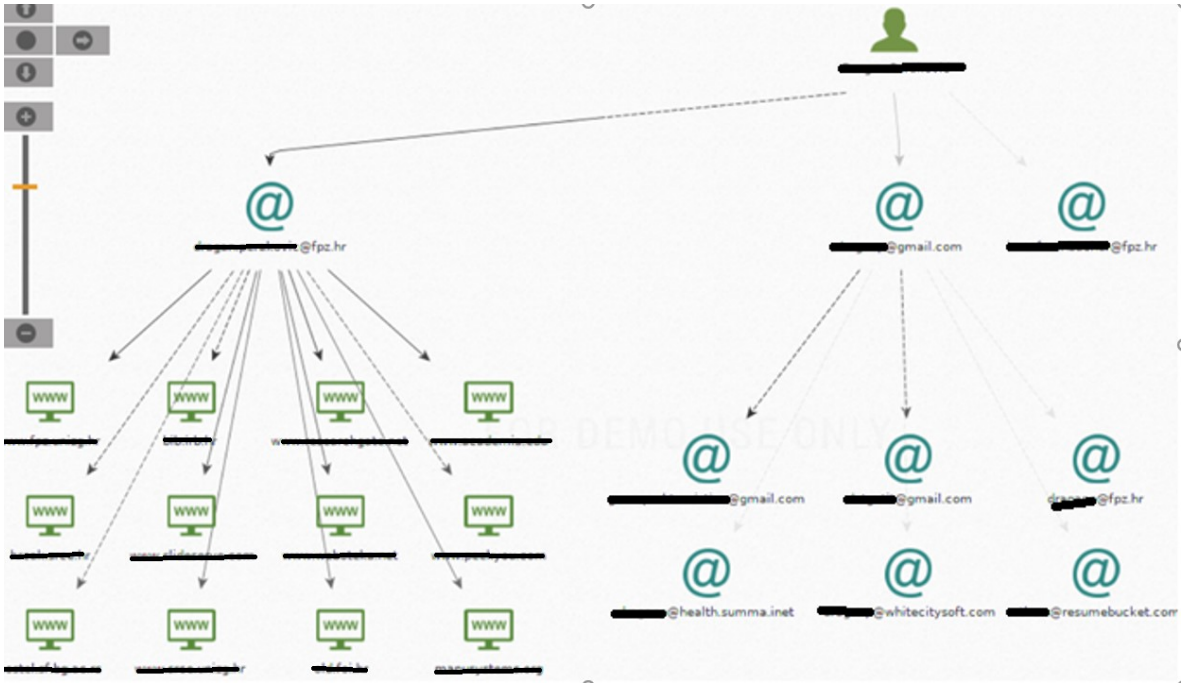
5.1.2.1. Automatizirano prikupljanje informacija o IK sustavu pomoću alata *Maltego*

Jedan od alata koji se koriste i znatno pomažu u ovoj fazi je *Maltego*. Isti se koristi kako bi se prikupile razne informacije. Koje su dostupne sa službenih internet stranica mete napada. Preko usklađenog lokatora sadržaja (*Uniform Resource Locator*, URL), on dolazi do raznih podataka o mreži koja se skenira. Osim za podatke o mreži, može se koristiti i za istraživanje ljudskog sektora koji se nalaze unutar određenog IK sustava. Alat je prikazan na slici 7. Ispod URL-a fakulteta, vidljiv je popis *email* adresa jednog dijela osoblja fakulteta.



Slika 7. Rezultati email adresa pomoću Maltega

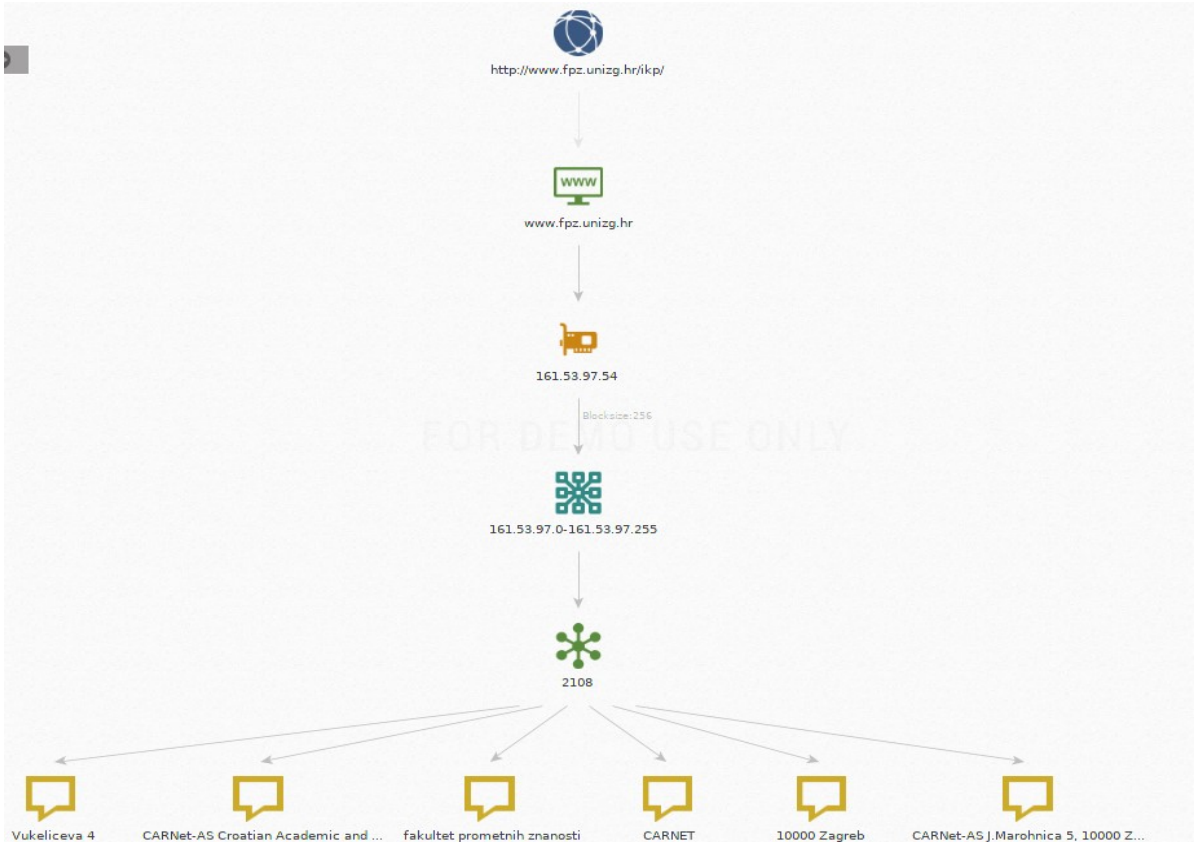
Primjer detaljnijeg istraživanja pojedinca vidi se na slici 8. Ona prikazuje rezultate pretrage upita o jednom visoko pozicioniranom zaposleniku. Osim prikaza poznate *email* adrese koja se koristi za potrebe fakulteta, prikazan je i vjerojatno, privatan *mail* *******@gmail.com uz kontakte s kojima je komunicirano. Ispod službenog maila nalazi se skup često pristupanim stranicama pomoću korisničkog računa.



Slika 8. Pretraživanje osobe pomoću Maltega

Ovakvi podaci možda se čine nebitnima, međutim vrlo su korisni za postupak naziva socijalni inženjering. U njemu se isti, mogu koristiti za dodatno ugrožavanje sustava na način iskorištavanja njegovog ljudskog faktora, koji je često najranjiviji element IK sustava.

Pomoću URL-a dobiva se bolji uvid u mrežnu hijerarhiju fakulteta uz dodatne informacije o njemu, slika 9.

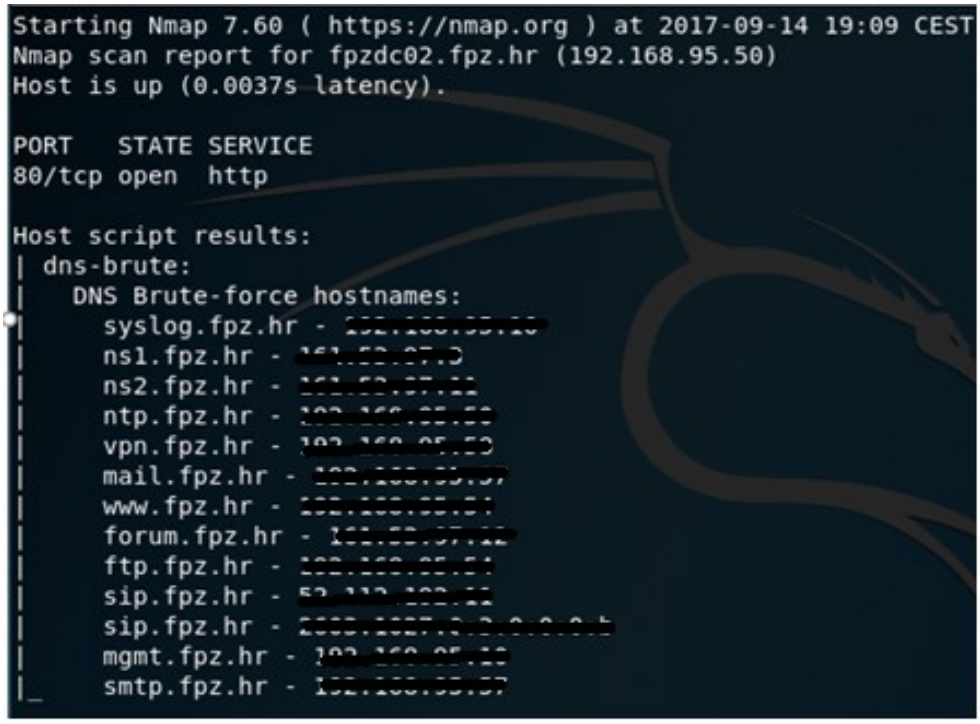


Slika 9. Maltego hijerarhija fakulteta

Na dnu Maltego grafa, nalaze se informacije o fizičkim lokacijama poput glavne zgrade fakulteta u Vukelićevoj 4 i adresa CARNeta u Marohnićevoj 5, 10000 Zagreb. Također, uočava se i doseg IP adresa fakulteta (161.53.97.0 – 161.53.97.225), koja sadrži i adresu *web* poslužitelja fakulteta. Na poslužitelju se nalazi domena www.fpz.unizg.hr i stranica smjera IKP.

5.1.2.2. Korištenje alata *Nmap* za prikupljanje informacija o mreži IK sustava

Alat naziva *Nmap* (*Network Mapper*), inače se koristi u fazi skeniranja mreže za provjeru portova ili usluga koje koristi računalo, no može koristiti i za prisilnu ekstrakciju podataka iz DNS-a (DNS *bruteforce*). Rezultati *Nmap* modula za skriptiranje (*Nmap Scripting Engine*, NSE) u obliku DNS *bruteforce* naredbe su prikazani slikom 10. Na se njoj vidi popis pod mreža fakulteta i pripadajućih IP adresa. Informacije prikupljene ovim putem se koriste kako bi se proširio obuhvat djelovanja u sljedećem koraku.



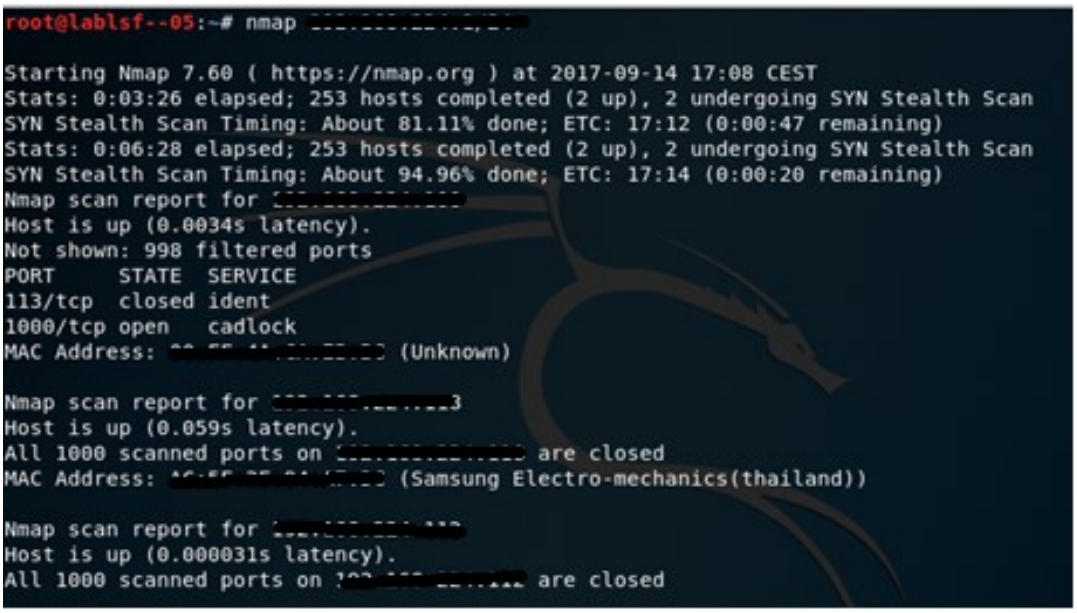
Slika 10. DNS bruteforce

Otkrivene pod domene su poslužitelji za poštu, forum, VPN i internet stranicu fakulteta, FTP i drugi. Svi otkriveni poslužitelji mogu biti podvrgnuti dodatnoj detekciji ranjivosti i iskorišteni za povećavanje uspješnosti testa. Međutim opseg takvog testiranja bi uvelike povećao trajanje i složenost penetracijskog testa u radu.

5.1.3. Otkrivanje ranjivosti skeniranjem mreže

Prilikom provedbe ovog koraka testiranja, ne izvršava napad ali se pokreće ne standardna korisnička aktivnost s ciljem identificiranja potencijalnih ranjivosti u ciljanom okruženju. Unutar mreže otkrivaju se uređaji uz pomoć prethodno skupljenih podataka poput IP adresa *hostova*.

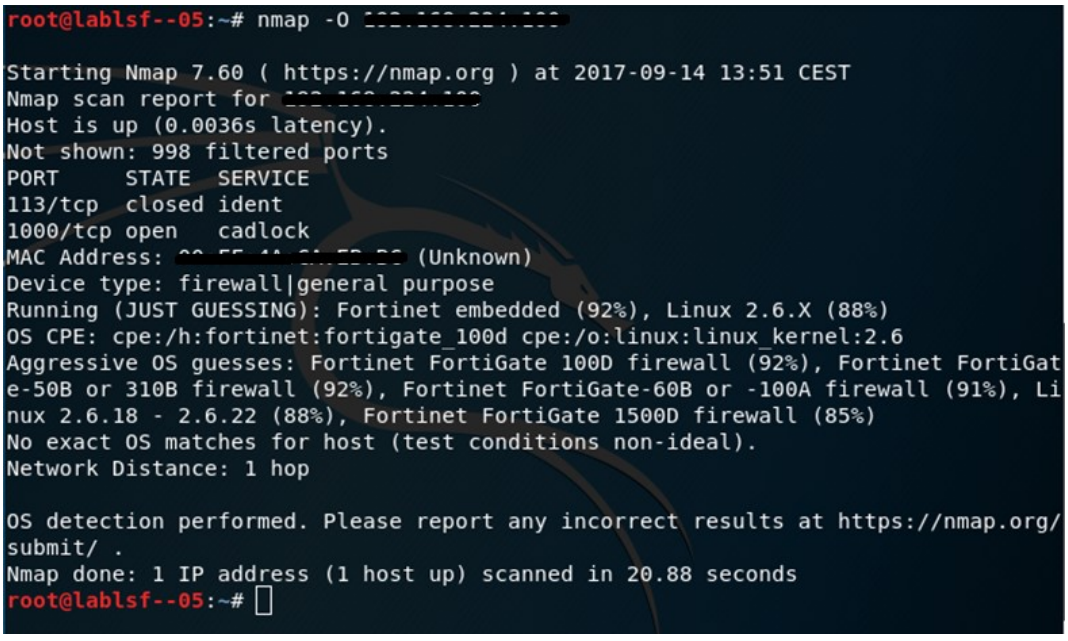
Skeniranjem mreže lociraju se aktivna računala koja mogu biti napadnuti u sljedećoj fazi. Za ovaj postupak korišten je alat *Nmap*. Njime je skenirana pod mreža na kojoj se nalazi AP, vidljiv na slici 11, s ciljem identifikacije aktivnih računala. Naredba vraća informacije o uređajima koji su dostupni na mreži.



Slika 11. Skeniranje podmreže

Nmap otkriva informacije o korištenim IP adresama, MAC adrese i nazive proizvođača (ako je to moguće), dostupne *portove* te usluge koje se koriste. AP laboratorija koristi tzv. „*client side isolation*“ postavku koja bežičnim klijentima ne dopušta međusobnu komunikaciju već samo komunikaciju s AP-om. Zbog tog razloga klijentov *laptop* je nevidljiv te se ne pojavljuje u rezultatima skeniranja.

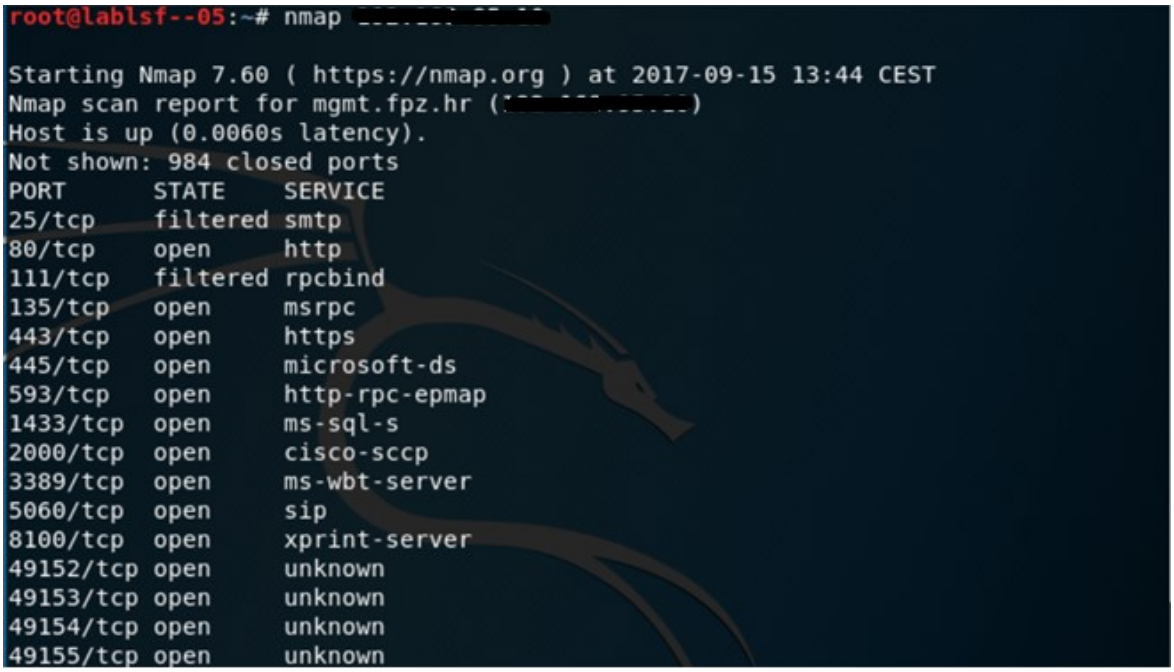
Osim skeniranja cijele podmreže, moguće je definirati i skenirati točno određenu IP adresu te, vidljivo naredbom na slici 12. Pomoću naredbe za otkrivanje verzije OS-a, može se dobiti više informacija o uređaju koji tu adresu koristi.



Slika 12. Skeniranje određenog računala u mreži

Ova naredba radi što je moguće točniju analizu uređaja, te je uz *portove* moguće vidjeti i detalje o MAC adresi, tipu uređaja i imenu te softvera koji se koristi. *Nmap* je nakon pokretanja naredbe identificirao vatrozid *Fortigate* zbog toga što na preklopniku on filtrira sav promet te se odgovara na upite *Nmap*-a umjesto AP-a. Identifikacija OS-a ponekad nije moguća sa 100% točnom verzijom, stoga program to nadoknađuje ponudom sličnih rješenja koja odgovaraju u postotcima.

Nmap se zatim koristi za skeniranje adrese jedne podmreže fakulteta, koja je odabrana pomoću rezultata DNS *bruteforca*, na primjeru sa slike 13 odabran je syslog.fpz.hr.



Slika 13. Skeniranje *syslog-a*

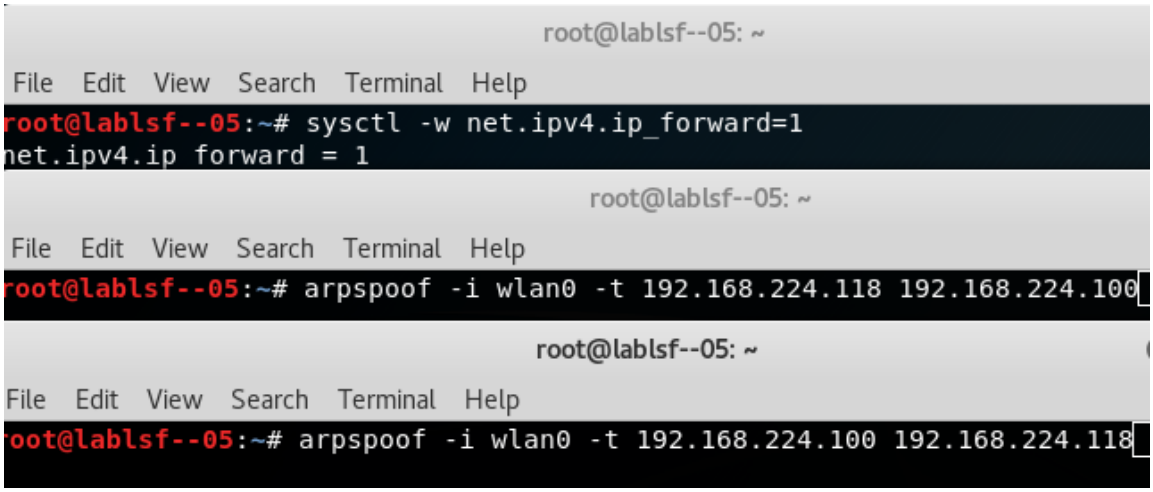
Nakon završetka skeniranja, iz rezultata koje je ponudio *Nmap*, vidi se da isti sadrži veliki broj otvorenih portova te se čini kao idealna lokacija za izvršavanje napada, međutim naglasak ovog potpoglavlja je bežična mreža laboratorija.

5.1.4. Iskorištavanje ranjivosti

Kao metu napada za potrebe rada odabire se pametni telefon. Za dokazivanje ranjivosti u mreži, odradit će se MITM koji se temelji na presretanju mrežnih paketa između pametnog telefona i AP-a, posredstvom *Kali* računala. Ovim postupkom napadač može ugroziti komunikaciju te analizirati mrežni promet koji se između njih razmjenjuje s ciljem daljnjeg kompromitiranja korisnika i sustava [34]. Napad je izravan udar na osnovno načelo povjerljivosti podataka unutar IK sustava.

Napad se temelji na trovanju ARP predmemorije (ARP *cache poisoning*) koja iskorištava nedostatak sigurnosnih mehanizama ARP protokola. Ova slabost, na drugom sloju OSI modela, omogućuje slanje upita o mrežnim adresama okolnih računala i dobivanja odgovora u WLAN mreži.

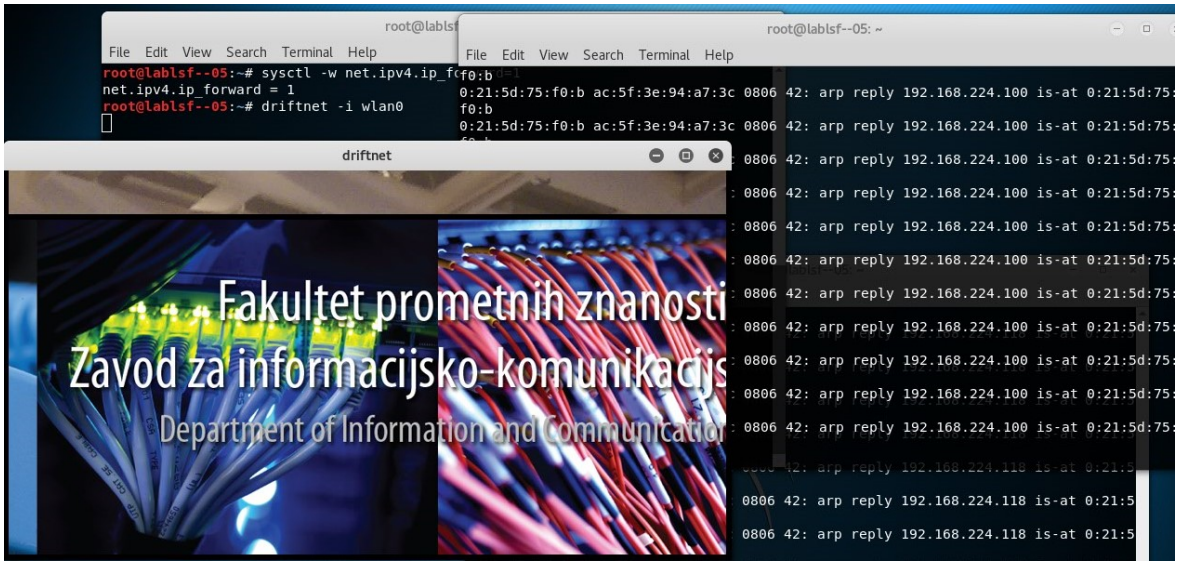
Kako bi se omogućilo prosljeđivanje mrežnog prometa između napadača (Kali računala) i mete (pametnog telefona), na Kali računalu potrebno je upaliti mrežnu mogućnost, naziva prosljeđivanje paketa (*packet forwarding*). Postupak po izvoru [35], započinje sintaksom koja se vidi na slici 14. Postiže se naredbom *sysctl*, koja privremeno omogućuje usmjeravanje paketa preko Kali računala. Isto služi kao lažni usmjerivač u WLAN mreži fakulteta.



Slika 14. *Arpsoof* sintaksa

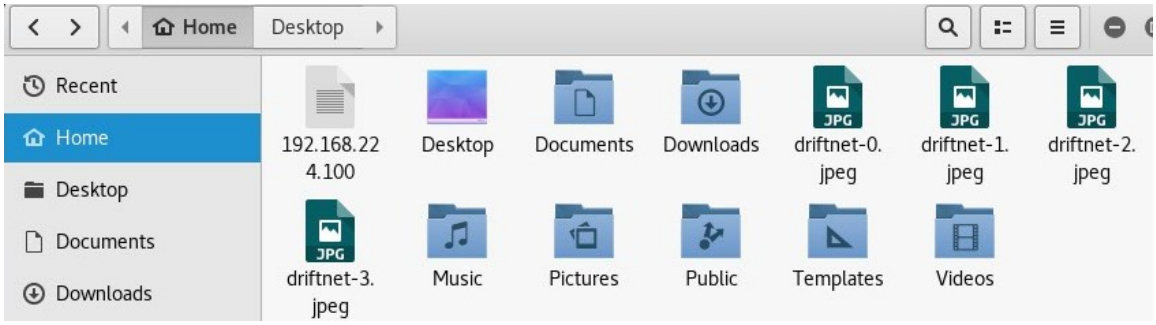
Nakon omogućavanja prosljeđivanja paketa, kako bi se Kali računalo moglo upotrijebiti kao posrednika u komunikaciji između mete i AP-a, potrebno je lažirati IP adrese odredišta pametnog telefona i AP-a. To se postiže uz pomoć naredbe *arpsproof* i sintakse vidljive na slici 14. Na ovaj način se mijenja upis u ARP predmemoriji, te se sav mrežni promet namijenjen pametnom telefonu, kreće preko Kali računala do AP fakulteta. Obrat tj. odgovor AP-a prema pametnom telefonu prolazi istim putem.

Nakon pokretanja naredbi, u različitim Kali terminalima, pokreće se i naredba *driftnet*, koja otvara prozor vidljiv na slici 15.



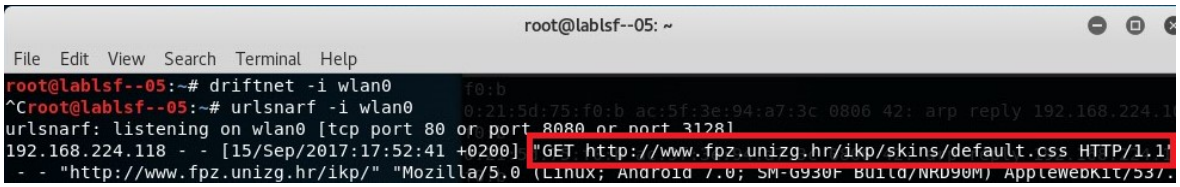
Slika 15. *Driftnet* prozor

Slika prikazana u okviru alata *driftnet* zapravo je prikazuje slikovni sadržaj kojem je u tom trenutku bilo pristupljeno na internet pregledniku pametnog telefona. Kali laptop, prikazuje sliku jer je ona prenesena od AP do telefona preko njega. Napadač cijelo vrijeme vidi ono što i korisnik preko vlastitog terminalnog uređaja, a sve slike koje se pregledaju, spremaju se u *.jpeg* formatu na radnoj površini Kali računala, slika 16.



Slika 16. Pregled korisnikovih slika

Izvedba ovog napada u mreži može biti korisna za prikupljanju novih, vrjednijih informacija poput lozinki i korisničkih imena koja se preko AP-a povezuju u mrežu. Isti bi se potom koristili za dodatno ugrožavanje sustava. Osim navedenog, napad može biti iskorišten i za pregledavanje trenutnih internet stranica koje korisnik posjećuje, vidljivo na slici 17. Na njoj se primjećuje još jedan sigurnosni nedostatak odnosno uporaba HTTP-a umjesto sigurnijeg proširenja HTTPS (HTTP *Secure*) za potrebe službenih *web* stranica fakulteta.



Slika 17. URL mete

Pomoću ove jednostavne ranjivosti na drugom sloju OSI modela, moguće je ugroziti korisnike IK sustava prisluškivanjem te prikupljanje raznovrsnih informacije poput različitih korisničkih računa i lozinki, pinova, *email* poruka itd.

5.1.5. Pivotiranje i izvlačenje podataka iz testiranog IK sustava

Dosad navedeni koraci, ponavljali bi se kroz navedene iteracije s ciljem prikupiljanja informacija potrebnih za dokazivanje i provođenje napada koji bi učinio maksimalnu štetu testiranom IK sustavu.

Svakom iteracijom, napadač proširuje informacije o sustavu te povećava razinu ovlasti tj. od ne autenticiranog korisnika koji se slučajno našao u sustavu, dolazi se do razine ovlasti koje imaju administratori mreža sustava. Postupak sam po sebi traje tjednima a ponekad i mjesecima.

5.1.6. Izvještavanje o slabostima pronađenim u laboratoriju

Pristupanjem AP-u, utvrđeni su sigurnosni nedostaci primjene neke od metoda zaštite u WLAN mrežama. Preporuka je postaviti barem WPA ili WPA2 oblik enkripcije a u budućnosti uvesti uporabu WPA3 standarda.

Nakon pronalaska terminalnog uređaja, isti je napadnut MITM napadom, temeljenim na presretanju mrežnih paketa između pametnog telefona i AP-a, kojeg omogućuje ranjivost naziva trovanje ARP predmemorije.

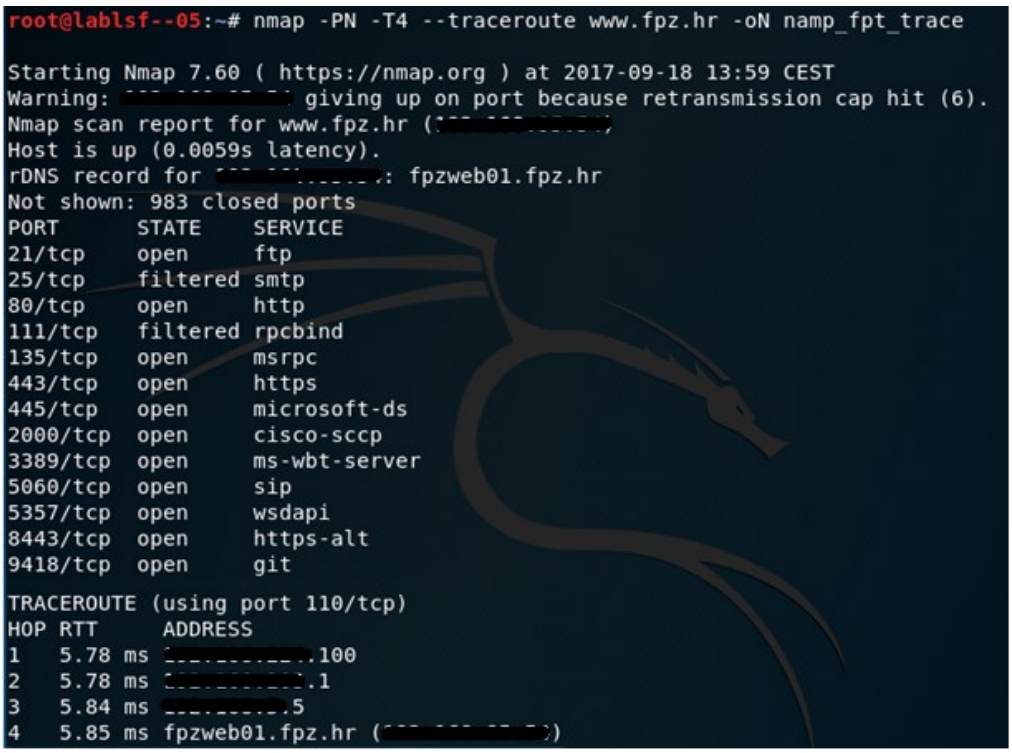
Detaljno izvještavanje o informacijama dobivenim u laboratoriju bit će u sljedećem poglavlju koje se bavi analizom dobivenih rezultata iteracija testiranja.

5.2. Druga iteracija validacije sigurnosti

Nakon ugrožavanja korisnika spojenih na AP, napadač se može posvetiti daljnjem istraživanju žične mreže s ciljem ugrožavanja ostatka IK sustava. Sljedeći podnaslovi opisuju informacije koje stoje na raspolaganju napadaču nakon povezivanja na AP i daljnje napredovanje kroz mrežu IK sustava.

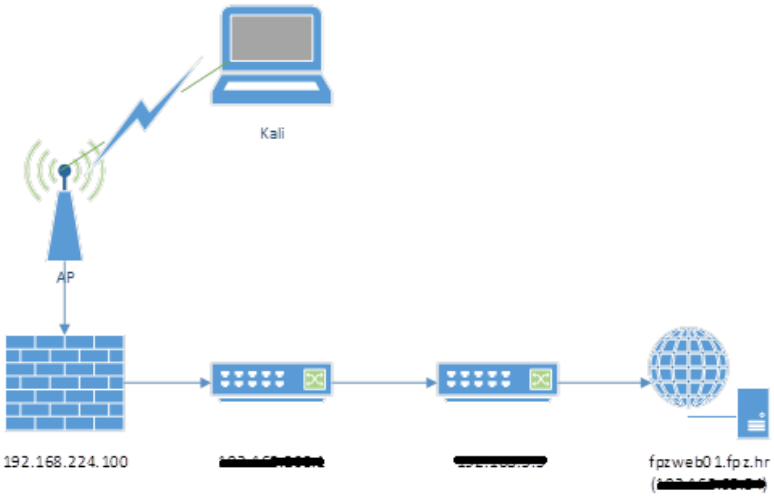
5.2.1. Aktivno prikupljanje informacija

Za skeniranje domene fakulteta ponovo se koristi već spomenuti *Nmap.* Slika 18 prikazuje rezultate upita čiji je cilj identifikacija IP adrese, naziva poslužitelja te potencijalno otvorenih portova koji su ranjivi na napad.



Slika 18. *Nmap* skeniranje domene

Uz nekoliko dodatnih postavki, dodana je i opcija --*traceroute* koja identificira broj mrežnih čvorova koje paket prolazi od izvorišta do odredišta. To je udaljenost koju paket prelazi od Kali računala do *web* poslužitelja fakulteta, preko mrežne infrastrukture fakulteta. Ovime je moguća identifikacija nepoznatih mrežnih čvorova. Ta informacija koristi se za izradu mrežnog dijagrama, vidljivog na slici 19.



Slika 19. Mrežni dijagram

Odgovor naredbe sa slike 18 donosi nove četiri IP adrese u mreži fakulteta te se zaključuje da su to mrežni čvorovi (vjerojatno usmjernici ili poslužitelji) koji vode do *web* poslužitelja fakulteta. Prateći ovaj dijagram, u ostatku poglavlja, obavljat će se detaljnije ispitivanje pronađenih čvorova u mreži.

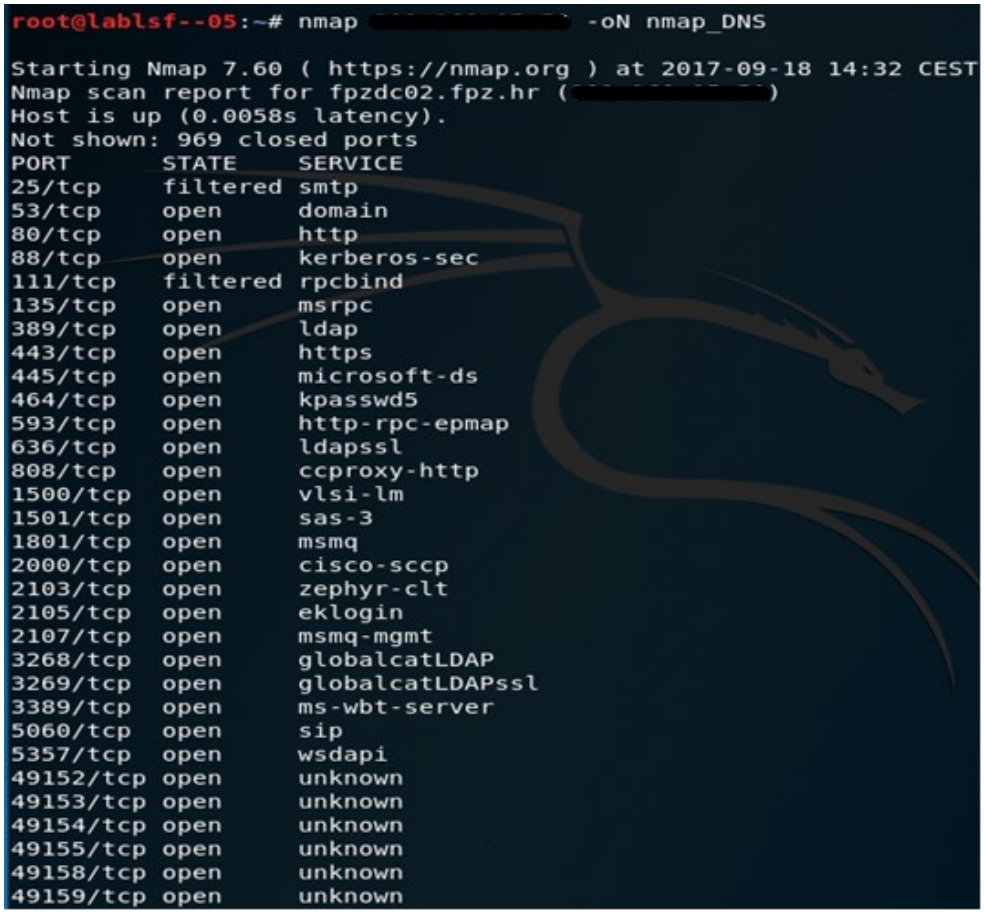
Alat koji se iskoristi za prikupljanje dodatnih podataka o domeni fakulteta je i *Whois.* Protokol odnosno upit *Whois*, vidljiv na slici 20, daje različite informacije o domeni, poput opisa tj. imena ustanove kojoj pripada, geografske adrese, oznake administratora te osobe na fakultetu koja je za nju zadužena.

```
root@lablsf--05:~# whois fpz.hr
domain:     fpz.hr
descr:      SVEUČILIŠTE U ZAGREBU FAKULTET PROMETNIH ZNANOSTI
descr:      Vukelićeva 4
descr:      10000 Zagreb
descr:      HR
admin-c:    C46760-HR
zone-c:     C46760-HR
expires:    20180320
source:     HR

person:     [redacted]
org:        Fakultet prometnih znanosti
nic-hdl:    C46760-HR
source:     HR
```

Slika 20. *Whois* fpz.hr

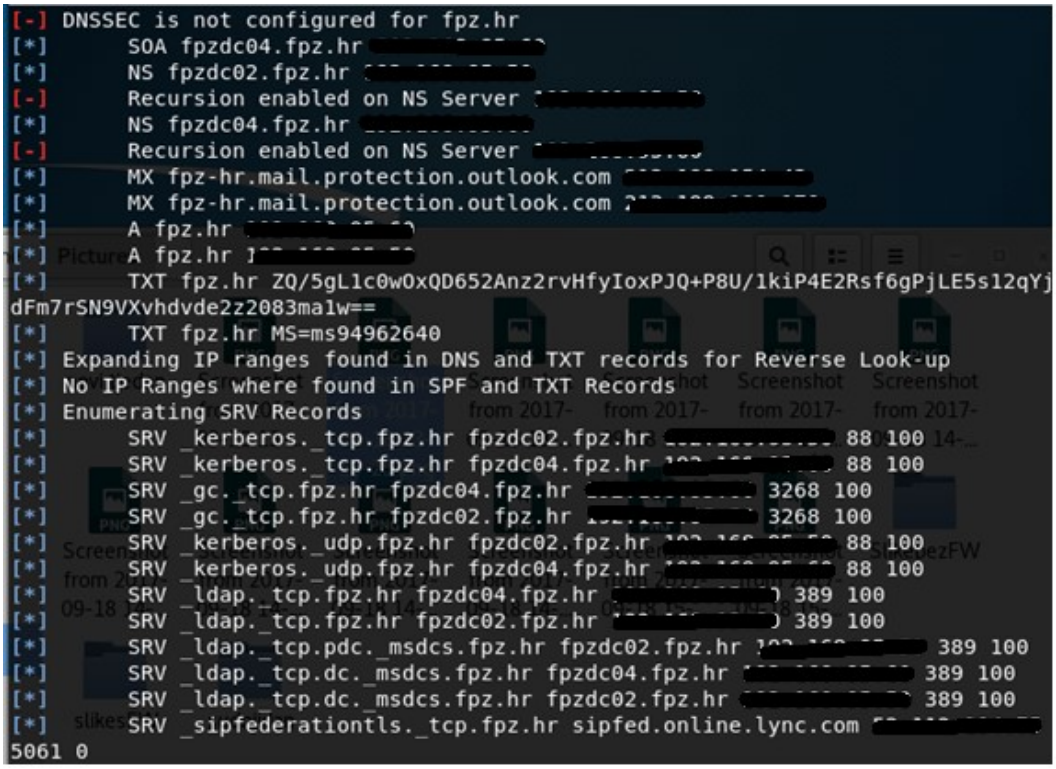
Skeniranje DNS-a sljedeći je korak zato što DNS može sadržavati mnogo korisnih informacija za napadača. Informacije koje se ovdje otkrivaju, vidljive na slici 21, odnose se na otvorene *portove* i usluge koje podržavaju.



Slika 21. Skeniranje DNS-a

Pomoći informacija prikupljenih iz DNS-a, iskusni tester ili pak zlonamjerni napadač, dobiva dovoljnu količinu informacija za razradu početnog plana ugrožavanja IK sustava. Na primjer, napadač bi se mogao fokusirati na TCP port 464, usluga *kpasswd* i pokušao ugroziti poslužitelja lozinki *Kerebros* sustava.

DNS *recon* je još jedan alat za dobivanje informacija iz DNS-a, koji javlja da *Domain Name System Security Extensions* (DNSSEC) nije konfiguriran te uzima podatke, slika 22.



Slika 22. DNS *recon*

Ovdje se mogu vidjeti informacije o zaštiti *mail* poslužitelja, te uporaba *kerberos* autentikacijskog protokola u mreži.

Još jedan od načina za dobivanje daljnjih meta napada može biti i naredba „nmap -sP -T4 fpz.hr/24 “ koja omogućuje detaljan uvid u računala dostupna na pod mreži (Tablica 3), uporabom *ping-a* za skeniranje *hostova*. Rezultati upita vraćeni su s imenom uređaja i pripadajućom IP adresom. Također je označena razina osjetljivosti ovih informacija prilikom testiranja.

Tablica 3. Podmreže fakulteta s pripadajućim nazivima, IP adresama i komentarom

***Host* ime**	**IP adresa**	**Razina Osjetljivosti**
mgmt.fpz.hr	1**.**8.95.10	Visoka
fpzc2h1.fpz.hr	1**.**8.95.21	Srednja
fpzh3.fpz.hr	1**.1**.95.23	Srednja
fpzc1h1.fpz.hr	1**.1**.95.31	Srednja
fpzdc02.fpz.hr	1**.1**.95.50	Srednja
fpzsql.fpz.hr	1**.1**.95.52	Visoka
fpzsql01.fpz.hr	1**.**8.95.53	Visoka
fpzweb01.fpz.hr	1**.1**.95.54	Umjerena
fpzexchange01.fpz.hr	1**.1**.95.57	Umjerena

fpzvpn01.fpz.hr	1**.1**.95.58	Visoka
fpzsc01.fpz.hr	1**.1**.95.59	Srednja
fpz.hr	1**.1**.95.60, druga DNS adresa: 1**.1**.95.50	Niska
fpzsccm.fpz.hr	1**.1**.95.61	Srednja
fpzweb02.fpz.hr	1**.1**.95.62	Srednja
fpzlic01.fpz.hr	1**.1**.95.63	Srednja
fpzmysql01.fpz.hr	1**.1**.95.66	Srednja
fpzbkp.fpz.hr	1**.1**.95.70	Srednja
fpzcopy02.fpz.hr	1**.1**.95.72	Umjerena
fpzvisum.fpz.hr	1**.1**.95.73	Srednja
fpzsordito.fpz.hr	1**.1**.95.75	Srednja
fpztest.fpz.hr	1**.1**.95.77	Srednja
fpzfinancije01.fpz.hr	1**.1**.95.78	Visoka
fpzprojekti.fpz.hr	1**.1**.95.79	Visoka
fpzur01.fpz.hr	1**.1**.95.200	Srednja

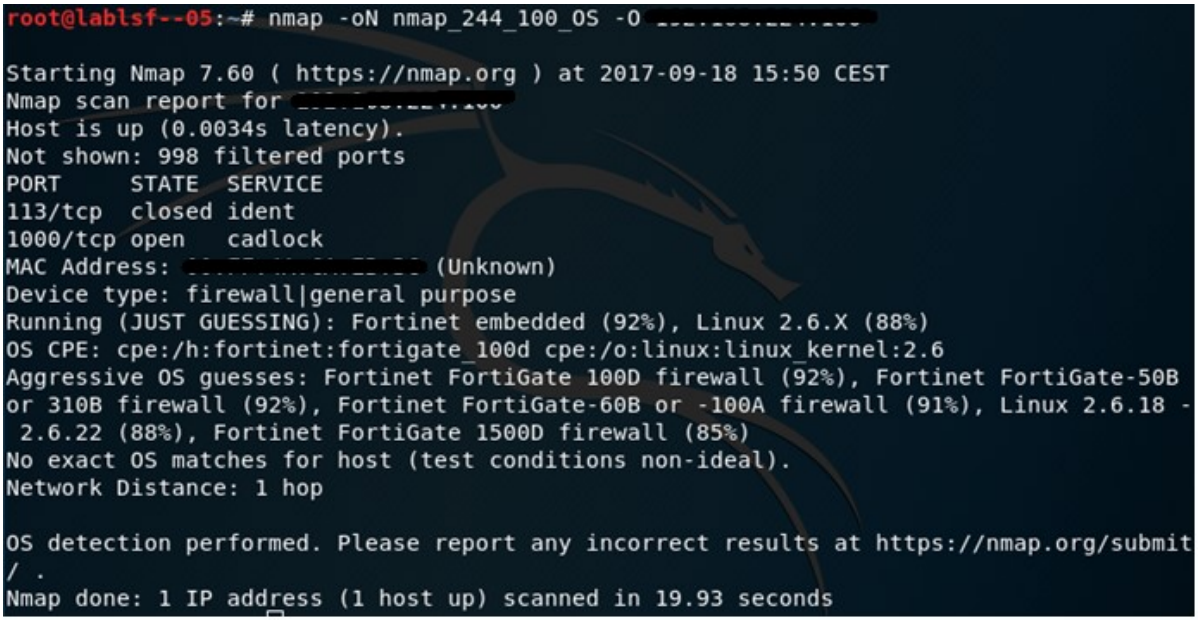
Ista je donesena po sljedećim kriterijima: niska razina označava javne poslužitelje fakulteta, srednja i umjerena razina označuju IP adrese unutar mreže fakulteta koji su privatni. Poslužitelji visoke razine osjetljivosti mogu poslužiti u sljedećoj iteraciji testiranja s ciljem pristupa tajnim informacijama fakulteta. Takve nisu zabilježene niti nađene jer se odnose na profesionalne oblike testiranja čija kompleksnost nadilazi doseg ovog rada.

5.2.2. Skeniranje mrežne rute

Podaci iz *traceroute* naredbe koristit će se za identifikaciju svih dijelova rute tj pripadajuće mrežne čvorove koji se nalaze na putu od terminalnog uređaja spojenog na AP, do web poslužitelja koji sadrži internet stranicu fakulteta.

5.2.2.1. Identifikacija prvog mrežnog čvora

Skeniranje podmreže kao rezultat daje samo IP adrese Kali računala i vatrozida. Detaljnijim upitom u *Nmap*-u, moguće je detektiranje verzije OS-a, još zvane i OS *fingerprint* za traženu IP adresu. Rezultati naredbe su prikazani slikom 23.



Slika 23. Skeniranje OS vatrozida

Iz dobivenih podataka moguće je odrediti više informacija o mrežnom elementu:

1. Tip uređaja (usmjerivač, radna stanica itd.) - Vatrozid
2. Pokreće (OS kojeg koristi) – ugrađeni Fortinet ili Linux 2.6.X
3. OS detalji (ime i verzija OS) – Fortigate 100 D, 60 B ili drugi
4. Mrežna udaljenost (udaljenost u skokovima (hops) između mete i napadača): 1 hop

5.2.2.2. Identifikacija drugog mrežnog čvora

Potajnim skeniranjem mreže (TCP *stealth scan*) naredbom "nmap -sS -T3 1**.1**.203.1/24" moguće je identificirati četiri *hosta*. Rezultati upita su vraćeni u obliku popisa IP adrese, opisom *porta* tj. stanjem i kraticom usluge (Tablica 4).

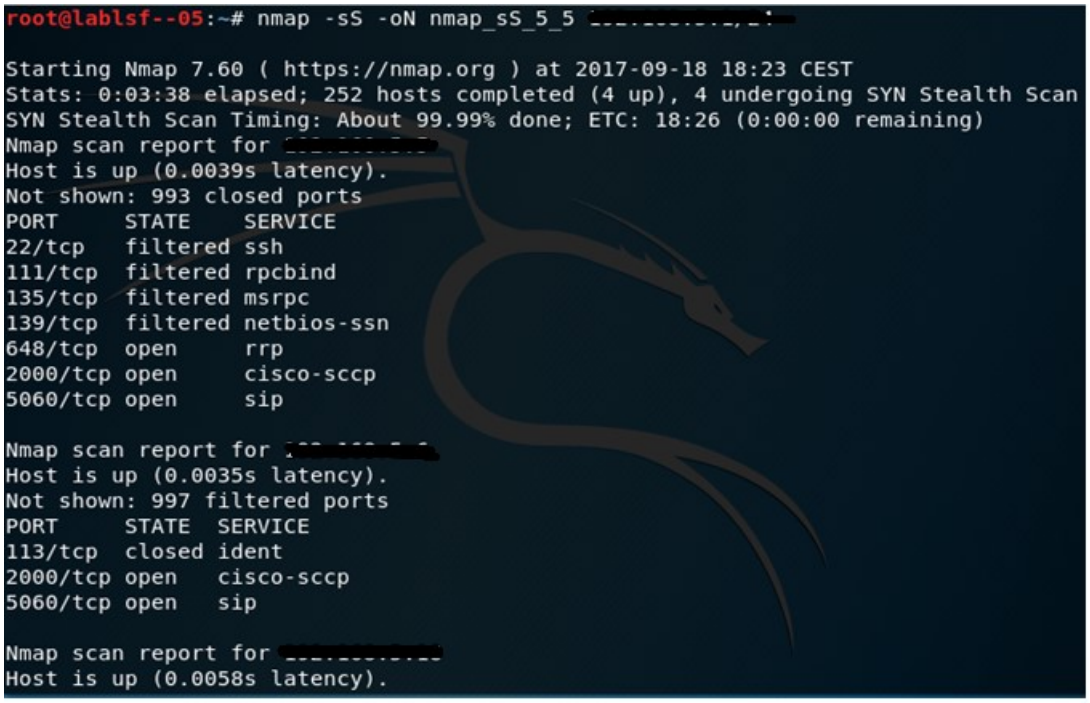
Tablica 4. Dostupna računala u mreži s pripadajućim informacijama poput IP adrese, broja i stanja porta te usluge.

IP adresa	*Port*	Stanje *porta*	Usluga
1.1**.203.1**	113/tcp 2000/tcp 5060/tcp	closed open open	ident cisco-sccp sip
1.1**.203.5**	2000/tcp 5060/tcp	open open	cisco-sccp sip

1.1**.203.91**	113/tcp	closed	Ident
	135/tcp	open	Msrpc
	139/tcp	open	netbios-ssn
	445/tcp	open	microsoft-ds
	902/tcp	open	iss-realsecure
	912/tcp	open	apex-mesh
	2000/tcp	open	cisco-sccp
	3389/tcp	open	ms-wbt-server
	5060/tcp	open	sip
	5357/tcp	open	wsdapi

5.2.2.3. Identifikacija trećeg mrežnog čvora

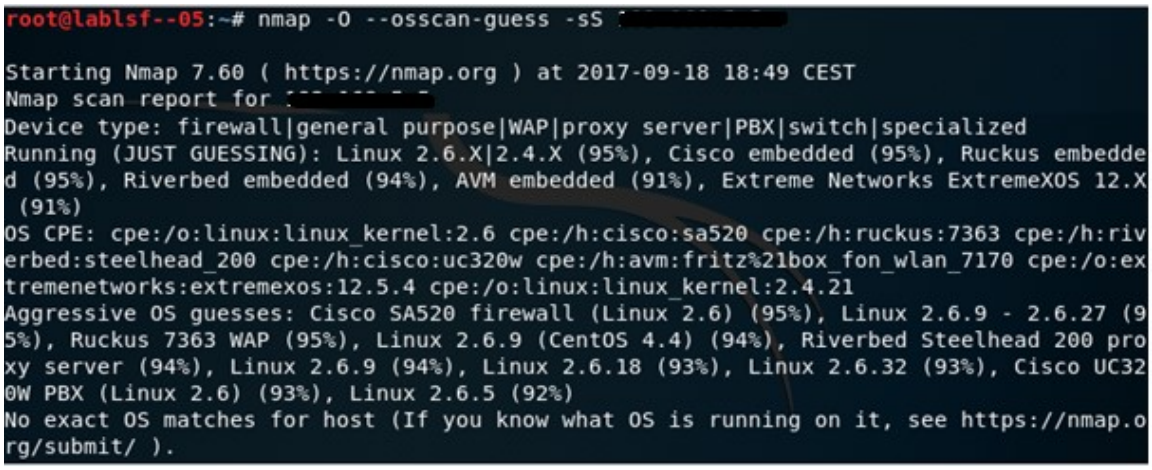
Prateći mrežni dijagram, uz pomoć Nmap-a skeniraju se sve dostupne podmreže čvora 192.168.5.1/24.



Slika 24. Skeniranje mrežnog čvora

Na slici 24 vidljiva je identifikacija mrežnog čvora 192.168.5.5, koji se koristi za put od laptopa do *web* poslužitelja Fakulteta, i ostalih *hostova* dostupnih na podmreži.

Daljnjim istraživanjem mogu se utvrditi namjene i OS koji čvor pogoni, slika 25, a po potrebi *Nmap* se može prisiliti da pokuša otkriti navedeno.

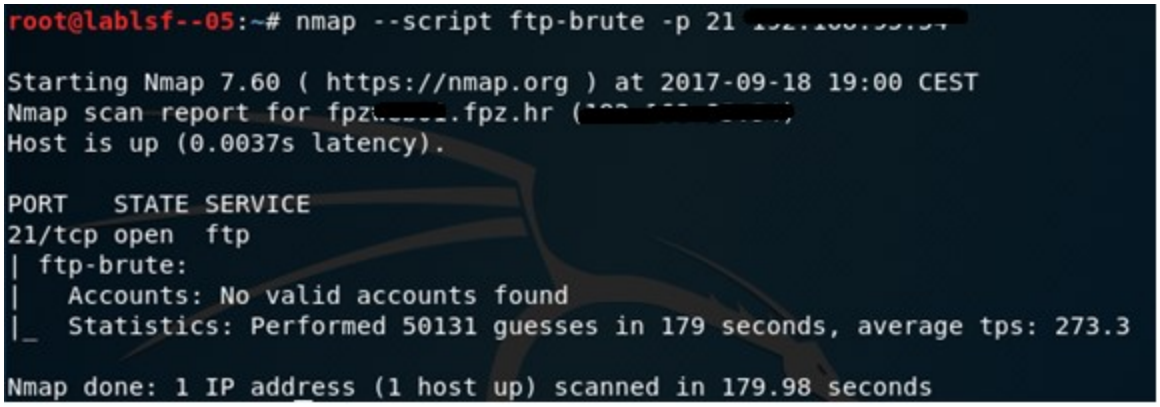


Slika 25. Naredba prisilnog pogađanja OS

Među rezultatima pretraga su vatrozid, *proxy* poslužitelj ili PBX sa softverom Linux 2.6.X te Cisco mrežni uređaj. Kao što je već rečeno, *Nmap*, kada nije siguran u procjenu uređaja, nudi popis mogućih rješenje izražen u postotcima koje odgovaraju skeniranom uređaju.

5.3.1. Provjera WEB poslužitelja

Princip rada Nmap-a sa *bruteforce* skriptom, vidi se na slici 26. Ova skripta provjera ranjivosti *web* poslužitelja preko FTP usluge i otvorenog porta 21.



Slika 26. FTP *bruteforce*

Prilikom izvršavanja skripte, nije nađen ni jedan korisnički račun koji bi omogućio ulaz na poslužitelj i time ugrozio sigurnost IK sustava fakulteta.

6. ANALIZA DOBIVENIH REZULTATA I PRIJEDLOZI UNAPRJEĐENJA ZAŠTITE

Ovo poglavlje bavi se analizom rezultata tj. podataka dobivenih za vrijeme provođenja testa u laboratoriju fakulteta i predlaganjem nekih metoda koje bi potencijalno unaprijedile razinu sigurnosti u laboratoriju.

6.1. Analiza rezultata prve iteracije testiranja

Potpoglavlje se bavi analizom rezultata dobivenih prilikom provedbe prve iteracije validacije sigurnosti IK sustava Fakulteta. Ona se bavi pregledom stanja AP-a koja ne koristi nikakav oblik enkripcije, dok za potrebe autentikacije u mreži od korisnika traži proizvoljan *email* račun. Radi preglednosti, isto je podijeljeno na sljedeća potpoglavlja: pregled dostupnih AP-a u dometu Kali računala, analiza informacija dobivenih pomoću alata *Maltego*, informacije dobivene korištenjem *Nmap* DNS *bruteforce* skripte, informacije dobivene skeniranjem bežične podmreže fakulteta alatom *Nmap* te napad na pametni telefon u bežičnoj mreži fakulteta.

6.1.1. Pregled dostupnih AP-a u dometu Kali računala

Prilikom identifikacije AP-a odobrenog za potrebe istraživanja rada, na slici 4, može se primijetiti osam otvorenih AP-ova i jednak broj onih kod kojih je korišten WPA2. Uz navedene, u dosegu se nalazi i pet mreža s oznakom MGT (*management*) koja označava uporabu WPA *Enterprise* metode zaštite.

Otvoreni AP-ovi su, uz *FreeWiFi* odnosno metu validacije sigurnosti, pretežito namijenjeni posjetiteljima kampusa u tzv. gostinjskim (*guest*) mrežama. Zbog toga ne koriste nikakve metode zaštite nego omogućuju slobodan pristup svima te su potencijalna opasnost za korisnike ali i za IK sustave u kojima se nalaze.

AP-ovi koji koriste WPA2 enkripciju pripadaju službenim podmrežama poput laboratorija Fakulteta ili drugo. Pregledavanjem BSSID-eva *FreeWiFi* i *lab_lsf*, može se doznati više informacija o potencijalno korištenoj infrastrukturi mreže fakulteta. Pomoću prva tri para znamenki BSSID-a moguće je ustanoviti kako je proizvođač AP tvrtka *Fortinet, Inc*. Također je vidljivo kako se ta dva ESSID-a odašilju s istog AP-a (sličan BSSID u prva četiri para znamenki), odnosno da se koristi više logičkih ESSID-a na jednom fizičkom uređaju. Ovime se postiže oblik mrežne segmentacije korisnika koji pomoću VLAN-a dijele fizički uređaj ali su međusobno logički odvojeni tj. pripadaju u različite podmreže Fakulteta.

MGT AP-ovi pripadaju *eduroam* mreži koju u velikom broju koriste studenti i ostali zaposlenici Sveučilišta na kampusu Borongaj koji imaju dodijeljene korisničke podatke tj. ime i lozinku za pristup mreži. Autentikacija korisnika provodi se uz uporabu nekog od pripadajućih poslužitelja poput RADIUS-a koji provjeravaju vjerodostojnost upisanih podataka te ovaj oblik predstavlja najveći način zaštite WLAN-a.

6.1.2. Analiza informacija dobivenih pomoću alata *Maltego*

Rezultat skeniranja s alatom *Maltego*, slika 7, prikazuje popis *email* adresa dijela osoblja fakulteta s pripadajućom domenom *@.fpz.hr.* Isti nisu pretjerano povjerljivi jer se mogu naći i na službenim stranicama fakulteta. Među njima se nalazi nekoliko privatnih *email* adresa s domena poput *@hotmail.com* i *@gmail.com* koje su privatnije te mogu poslužiti za *phishing* napade na vlasnike adresa.

Više informacija dobiva se upitom o točnom pojedincu, prikazanim na slici 8, sa zapisima često pristupanim *web* stranicama. Među njima se nalaze: *weboteka.net* koja sadrži veliki broj studentskih skripti i primjera ispita za potrebe studenata fakulteta, *manusystems.org* iza koje stoji međunarodna znanstvena konferencija naziva *International Conference on Management of Manufacturing Systems* na kojoj je meta pretraživana bila gost predavač. Dalje slijede stranica *postel.sf.bg.ac.rs* iza koje se nalazi „Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju“ organiziranog od Odseka za poštanski i telekomunikacioni saobraćaj, Saobraćajnog fakulteta u Beogradu i drugi.

Proučavanjem posjećenih stranica i interesima osobe zajedno s korisničkim *email*-ovima, poput onog od softverske kompanije „*WhiteCitySoft*“, napadač može napraviti oblik socijalnog inženjeringa naziva *spear phishing* te doći do povjerljivih informacija.

6.1.3. Informacije dobivene korištenjem *Nmap* DNS *bruteforce* skripte

Uporabom DNS *bruteforce* napada pomoću *Nmap* NSE-a, prikazan slikom 10, dobivaju se imena različitih računala priključenih na mrežu fakulteta. Isti čine osnovu mrežne infrastrukture te sadrže informacije koje se mogu upotrijebiti u sljedećim iteracijama testiranja. Može se primijetiti kako različita imena računala pokazuju na istu IP adresu. Razlog tome je vjerojatno uporaba više virtualnih poslužitelja na istom fizičkom poslužitelju.

Tako na primjer, napadač na IK sustav može pokušati ugroziti *syslog* ili *mgmt* poslužitelja koji sadrže podatke o svim događajima na mreži fakulteta [36]. Ovo računalo napadač bi ugrozio nakon povećanja razine pristupa, odnosno nakon što prisluškivanjem mreže, čitanjem *email*-ova ili *phishingom* zaposlenika fakulteta dobije korisnička imena i lozinke. Nakon pristupa zapisima s mreže, napadač ih može modificirati te sakriti svoje tragove od autoriziranog osoblja. Takvim postupkom bi utjecao na povjerljivost i integritet *syslog* zapisa a time i integritet ostatka IK sustava.

Sljedeća dva poslužitelja koji nose naziv *ns*, skraćeno za imenske poslužitelje (*name server*) odnosno računala koja obavljaju proces pretvorbe čovjeku razumljivih imena u IP adrese, te tako čine jedan od glavnih dijelova DNS-a svakog IK sustava [37]. Pristupom i modifikacijom istih, napad može utjecati na dostupnost mrežnih usluga fakulteta te tako narušiti još jedno načelo sigurnosti IK sustava.

Ako zadobije ovlasti nad *mail* i *smpt* poslužiteljima, čije se adrese također nalazi među dobivenim podacima, napadaču se nudi mogućnost nadzora sve mrežne komunikacije između korisnika *email*-a fakulteta. Ovakav scenarij dovodi do ozbiljnog ugrožavanja načela povjerljivosti te može poslužiti za potrebe *spear phishinga* ili čitanja pošte u potrazi za

informacijama poput korisničkih imena i lozinki. Posljedice su ugrožavanje povjerljivosti i cjelovitosti informacija u sustavu dok se s vremenom mogu proširiti i na dostupnost informacija u IK sustavu.

U dobivenim rezultatima nalazi se i adresa službene internet stranice i *ftp* poslužitelja fakulteta. Uspješan napad utjecao bi na cjelovitost informacija objavljenih na internetskim stranicama fakulteta dok bi se modifikacijom dokumenata utjecalo na cjelovitost i povjerljivost.

6.1.4. Informacije dobivene alatom *Nmap*

Slika 11 prikazuje naredbu i rezultate skeniranja AP fakulteta pomoću alata *Nmap*. Dobivene su informacije o dvije IP adrese koje se nalaze u podmreži. Iz jedne se identificira pametni telefon marke Samsung i to na temelju MAC adrese uređaja.

Identifikacija druge IP adrese, provodi se upitom u *Nmap*-u vidljiv na slici 12. Rezultati upita vraćaju informacije da je riječ o *Fortinet FortiGate* vatrozidu koji se koristi u laboratoriju fakulteta. Ovime se može utjecati na sigurnost IK sustava tako da napadač, nakon analize ranjivosti navedenog uređaja, isti onesposobi te tako olakša napredak kroz mrežu.

Korištenjem *Nmap*-a za skeniranje adrese *syslog* poslužitelja, prikazanim na slici 13, dobivaju se podaci o broju i vrsti porta, stanju te vrsti mrežne usluge koju poslužitelj pruža. Među identificiranima su *smpt*, *http*, *https*, usluge *microsoft directory* i drugi. Isti sadrži veliki broj otvorenih portova te se čini kao meta koju bi napadač mogao odabrati u kasnijim iteracijama napada.

6.1.5. Napad na pametni telefon u bežičnoj mreži fakulteta

Simulacijom napada na pametni telefon, dokazana je ranjivost uporabe otvorenog AP-a te je izvršen MITM napad. Napad je temeljen na trovanju ARP predmemorije (ARP *cache poisoning*), odnosno ranjivosti koja se nalazi u ARP-u [35].

Proces mrežne komunikacije između dva uređaja A i B, koje predstavljaju terminalni uređaj i AP ili drugi terminali koji se nalazi istom segmentu LAN-a, odvija se uz pomoć ARP tablica u kojima se nalaze pohranjeni podaci o IP i MAC adresi uređaja koji ih okružuju. Ako se na mreži nalazi i uređaj C, on može utjecati na ARP predmemoriju uređaja A i B, odnosno u tablice dodavati lažne IP i MAC adrese za uređaje A i B, zbog kojih komunikacija između njih ide preko uređaja C [38].

Lažiranje ARP tablica (ARP *spoofing*) je tehnika kojom napadač može napraviti izmjene zapisa u predmemoriji tako da zamijeni vrijednosti MAC i IP adresa u tablicama AP-a i pametnog telefona te komunikacijski kanal proširi s Kali računalom kao posrednikom u komunikaciji.

Osim demonstriranog MITM napada, ARP *spoofing* se može upotrijebiti i za provođenje napada uskraćivanjem usluge (*Denial of service, DoS*) te oponašanje uređaja (*Host impersonation*).

6.2. Analiza rezultata druge iteracije testiranja

Nakon pristupa i analize WLAN-a fakulteta, prelazi se na drugi dio testiranja odnosno kratkog uvida u koje informacije je moguće prikupiti nakon povezivanja na AP te istraživanja žičane mrežne infrastrukture fakulteta. Podaci su komentirani u sljedećim potpoglavljima: Analiza DNS poslužitelja IK sustava i analiza mrežnih čvorova IK sustava.

6.2.1. Analiza DNS poslužitelja IK sustava

Alatom *Whois* dobivene su informacije o domeni fakulteta, slika 20., poput: informacije o domeni, opisa odnosno punog imena ustanove kojoj domena pripada, geografske adrese, oznake administratora, trajanju, izvoru te osobe na fakultetu koja je za nju zadužena. Isti mogu biti upotrebljeni u metodama socijalnog inženjeringa.

Detaljnim skeniranjem DNS poslužitelja, čiji je IP otkriven u prošloj iteraciji, dobivaju se informacije, vidljive na slici 21. One se odnose se veliki broj otvorenih *portova* i usluge koje su podržane a nisu otkriveni prethodnim skeniranjima.

Zbog nedostatka DNSSEC-a, alatom DNS *recon* dobiveni su podaci vidljivi na slici 22. Uz već poznate informacije o *ns* poslužiteljima, dobivena su dva nova poslužitelja pošte (*mail exchange*, MX), koji pripadaju *.outlook.com* domeni. Uz navedeno dobivene se informacije o zaštićenim *mail* poslužiteljima, te da IK sustav fakulteta na nekim poslužiteljima koristi *Kerberos* autentikacijske protokole.

Rezultati dobiveni i prezentirani u tablici 3, označni su po razinama osjetljivosti informacija: visoka, umjerena, srednja i niska. Svaka razina na određeni način utječe na osnovna načela sigurnosti, stoga su neke IP adrese namijenjene samo zaposlenicima fakulteta a ne i ostalim posjetiteljima. Smatra se da više razine osjetljivosti doprinose većem broju ugroženih načela ako mrežni uređaj bude napadnut od strane napadača.

6.2.2. Analiza mrežnih čvorova IK sustava

Uporabom *Nmap* naredbe sa slike 18, uz dodatak opcije --*traceroute* identificira se broj skokova koje paket prolazi od izvorišta do odredišta. Tako je za primjer uzeta *web* stranica Fakulteta a nakon završetka skeniranja dobivaju se rezultati o mrežnim čvorovima koji su na putu između Kali računala i *web* poslužitelja na kojem se nalazi stranica. Uz navedene čvorove i njihove IP adrese, detektiraju se i različiti *portovi* i pripadajuće usluge koje se nalaze na poslužitelju. Isti sadrži dva filtrirana, 11 otvorenih i 938 zatvorenih *portova*. Usluge s otvorenim *portovima* često su prve mete napada na IK sustav.

Skeniranjem prvog čvora u mreži dobivaju se rezultati prikazani slikom 23. Zaključuje se kako je riječ o vatrozidu u laboratoriju fakulteta, iz zato što je temeljen na Fortinet OS-u, a ostale karakteristike govore kako pripada Fortigate 100 D ili sličnoj seriji uređaja.

U rezultati dobivene za drugi i treći mrežni čvor pripadaju popisi IP adresa, opisi *porta* tj. stanje i kratica usluge. Identificiraju se vatrozid, *proxy* poslužitelj ili PBX sa softverom Linux 2.6.X ili Cisco mrežni uređaj, koji mogu biti iskorišteni za daljnje ugrožavanje IK sustava.

Nakon identifikacije čvorova, obavljena je provjera *web* poslužitelja s jednostavnom *ftp-brute* skriptom, prikazanim na slici 26. Prilikom izvršavanja skripte, nije nađen ni jedan korisnički račun koji bi omogućio ulaz na poslužitelj te ugrozio sigurnost poslužitelja.

6.3. Klasificiranje podataka dobivenih u laboratoriju

Klasifikacija podataka podijelit će se na tri razine (tablica 5), kako bi se opisali povjerljivi podaci i informacije dobiveni tijekom provođenja validacije sigurnosti:

1. Razina osjetljivosti 3 – ovdje će pripadati sve informacije koje bi omogućile proces izvođenja napada na IK sustav. Tu spadaju IP adrese, *portovi*, mrežne usluge, OS i verzije bitnijih poslužitelja te mrežnih čvorova fakulteta.
2. Razina osjetljivosti 2 - ovdje će pripadati sve informacije koje vjerojatno same po sebi ne bi uzrokovale štetu ali bi njihovo otkrivanje na neki način utjecalo na osobe ili dijelove mreže IK sustava.
3. Razina osjetljivosti 1– ovdje će pripadati sve informacije čije otkrivanje ne bi imalo nikakvog direktnog utjecaja na sustav ali bi mogle biti iskorištene za kasnije iteracije napada na sustav

Tablica 5. Klasifikacija prikupljenih podataka u tri razine osjetljivosti informacija

Razina 1	Razina 2	Razina 3
URL javno dostupnih *web* stranica fakulteta i IP adresa	Privatni *email* korisnički račun i kontakti koje sadrži	IP adrese privatnih poslužitelja fakulteta dobivene *brute force* naredbom na DNS sustav
Javne *email* adrese sa .fpz domene	Raspon IP adresa pod domenom fakulteta	Verzije OS i usluga koje koristi vatrozid u laboratoriju
URL-ovi edukacijskih *web* stranica koje koristi osoblje fakulteta	Slike i URL s terminalnog uređaja podvrgnutog MITM napadu	Popis *portova* mrežnih komponenti za sigurnost IK sustava
IP adresa i URL forum.fpz	IP adrese umjerene i srednje razine povjerljivosti iz tablice 3	Lozinke koje se potencijalno mogu prikupiti MITM napadom

Informacije iz treće razine smatraju se povjerljivima. Razlog tome je činjenica da podaci svrstani u tu skupinu sadrže informacije o IP adresama unutarnje infrastrukture

fakulteta te ne bi trebali biti dostupni svakome. IP adrese menadžmenta, financija ili projekata fakulteta mogu biti iskorištene prilikom napada na fakultet kako bi se prouzročilo neki oblik financijske štete ili ugrožavanja ugleda. U tome im pripomažu informacije poput OS vatrozida, te uz malo strpljenja i lozinke prikupljene MITM napadom u bežičnoj mreži.

Informacije iz druge razine smatraju se ograničenima. Privatni *email*-ovi, popis posjećivanih stranica i pregledavanja interesa zaposlenika, mogu se iskoristiti u metodi socijalnog inženjeringa naziva *spear phishing*. U istom, se na temelju skupljenih informacija, od žrtve pokušavaju izvući različite osjetljive informacije poput lozinki i korisničkih imena.

Informacije iz prve razine smatraju se javnim. Iste su svakodnevno dostupne korisnicima. One također mogu biti korištene za jednostavne oblike *phishing* napada na zaposlenike fakulteta.

Početniku ili osobi koja se ne razumije u proces penetracijskog testiranja, podaci iz bilo koje razine ne moraju predstavljati nikakvu informaciju niti omogućiti iskorištavanje iste s ciljem ugrožavanja IK sustava. Ista klasifikacija, stručnjaku iz ovog područja ili iskusnom napadaču, može predstavljati dovoljan skup informacija potrebnih za jedan precizan udarac koji može ozbiljno ugroziti sigurnost IK sustava.

6.4. Prijedlozi unaprjeđenja zaštite u laboratoriju fakulteta

Sigurnosna infrastruktura Laboratorija je na visokoj razini te unatoč nedostatku enkripcije na AP se postiže virtualna odvojenost klijenata u mreži korištenjem VLAN segmentacije za više BSSID-eva na istom fizičkom uređaju, čime se umanjuje mogućnost napada. Preporuka bi ipak bila koristiti WPA2 metodu zaštite do implementacije WPA3 sigurnosnog protokola za potrebe WLAN-a fakulteta. Navedeni će dodatno osigurati pristup i mrežu fakulteta.

Nedostatak je vidljiv u sigurnosnom propustu MITM napada koji omogućuje presretanje korisničkih podataka i može predstavljati veliki sigurnosni problem ako se u prijenosu otkriju osjetljivi podaci poput korisničkih imena, lozinki, OIB-a i sl. Isti se može ukloniti primjenom WIPS, koji obavještavaju administratore o slučaju zlouporabe ARP naredbe te preventivno djeluju na pokušaje napada. Još jedan način povećanja sigurnosti je i *Dynamic* ARP inspekcija, koja ocjenjuje ARP zahtjeve u mreži te odbacuje one s neobičnim upitima vezanih za IP i MAC adrese.

Drugi sigurnosni nedostatak je mogućnost izvlačenja informacija iz DNS poslužitelja zbog nedostatka DNS sigurnosnih ekstenzija (*Security Extensions*) tj. DNSSEC. Preporuka za povećanje razine sigurnosti je primjena navedene tehnologije usprkos činjenici da je implementacija iste nešto kompliciraniji proces.

7. ZAKLJUČAK

Nekada je snažno konfigurirana mreža mogla služiti kao zaštitni zid koji je osiguravao klijentska računala i odbijao napadače od unutarnjih dijelova IK sustava te su se izrazi poput informacijske sigurnosti i sigurnosti IK sustava smatrali sinonimima. Danas to više nije moguće iz razloga što postoji previše ulaznih točaka koje se koriste u svrhu zaobilaženja sigurnosnih mjera mreže te olakšavaju napade. Uz to postoje i razne poteškoće koje se susreću prilikom obrane od tih napada poput univerzalno spojenih uređaja, povećane brzine i sofisticiranosti napada, dostupnosti te jednostavnosti uporabe alata za napad i bržeg otkrivanje ranjivosti.

Informacijska sigurnost je proces održavanja informacija i podataka u stanjima cjelovitosti, povjerljivosti i dostupnosti. To je proces koji nikada ne može biti završen, iz razloga konstantnih nastajanja novih prijetnji kojima je sustav izložen.

Sigurnost IK sustava je područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi sigurnosti klasificiranog i neklasificiranog podatka koji se obrađuje, pohranjuje ili prenosi u IK sustavu te zaštite njegove cjelovitosti, povjerljivosti i dostupnosti.

Klasificiranje je postupak određivanja vrijednosti različitim vrstama podataka i informacijama s ciljem procjene potrebne količine novca i resursa koji će biti namijenjeni njegovoj zaštiti.

Nakon dugogodišnjeg razvoja, bežične lokalne računalne mreže danas nalaze primjenu u velikom broju okruženja te iako donose mnoge prednosti, predstavljaju najslabiju kariku u mrežnom elementu IK sustava. Uz postojeće tri generacije zaštite (WEP, WPA i WPA2) i dalje je moguće izvođenje napada na sustave koji koristi ovakav oblik mrežne komunikacije. WLAN napadaču omogućuje neovlašten pristup IK sustavu, preko kojeg može uzrokovati štetu ili doći do raznih osjetljivih informacija koje se u njemu nalaze. Rješenja su primjena WPA2 uz snažne lozinke, uporaba VLAN segmentacije korisnika, mrežni uređaji za sigurnost poput vatrozida koji filtrira izlaz sa AP te uporaba WIPS tehnologije, koja proučava mrežni promet WLAN-a Mnogo se očekuju i od nadolazeće četvrte generacije metoda za zaštitu u WLAN mrežama, naziva WPA3.

Validacija sigurnosti ili penetracijsko testiranje je tehnika procjene trenutnog stanja sigurnosti IK sustava, temeljena na oponašanju stvarnog napada. Za vrijeme provođenja testiranja, ispitivač provjerava ciljani IK sustav izvodeći različite vrste napada istim tehnikama, alatima i načinom razmišljanja kakve bi koristio i stvarni zlonamjerni napadač na sustav. Jedan od glavnih ciljeva postupka je uočavanja bilo kakvih ranjivosti koje je moguće iskoristiti za ostvarenje neovlaštenog pristupa ili ugrožavanje sustava.

Pojam tradicionalnog penetracijskog testiranja postaje sve teže definirati, zbog mnogih različitih definicija koje su se s vremenom počele upotrebljavati za opisivanje različitih oblika sigurnosnih procjena. Dio ove tržišne zabune je zbog činjenice da se izraz "penetracijsko testiranje" danas više koristi za penetracijski test na temelju usklađenosti a ponekad čak i kao sinonim za procjenu ranjivosti IK sustava.

Informacije dobivene u laboratoriju klasificirane su u tri razine ovisno o njihovoj osjetljivosti. Informacije treće razine smatraju se povjerljivima te među njih pripadaju informacije o IP adresama unutarnje infrastrukture fakulteta poput adrese poslužitelja menadžmenta, financija ili projekata fakulteta koje mogu biti iskorištene za postizanje financijske štete ili ugrožavanja ugleda. Napadu pomažu informacije poput OS vatrozida, te potencijalne lozinke prikupljene MITM napadom u bežičnoj mreži. Informacije druge razine smatraju se ograničenima te sadrže privatne *email*-ove i popis *web* stranica koje daju uvid u interes zaposlenika. Isti se mogu iskoristiti u metodi socijalnog inženjeringa *spear phishing* za dobivanje različitih osjetljivih informacija poput lozinki i korisničkih imena promatranog IK sustava. Informacije prve razine smatraju se javnim te su svakodnevno dostupne korisnicima ali mogu biti korištene za jednostavne oblike *phishing* napada na zaposlenike fakulteta.

Glavni sigurnosni nedostatak promatranog AP je nedostatak enkripcije te mogućnost izvođenja MITM napada u nezaštićenim WLAN mrežama. Kako bi se spriječilo presretanje korisničkih podataka odnosno otkrivanje osjetljivih informacija poput korisničkih imena, lozinki i OIB-a, preporučuje se uporaba WPA/WPA2 metoda zaštite te primjena WIPS-a. On obavještava administratore o slučaju zlouporabe ARP naredbe te preventivno djeluje na pokušaje napada. Drugi sigurnosni nedostatak je mogućnost izvlačenja informacija iz DNS poslužitelja a preporuka za zaštitu je implementacija DNSSEC tehnologije.

LITERATURA

[1] Ciampa, M.: CompTIA® Security+ Guide to Network Security Fundamentals, Fifth Edition, Cengage Learning, Boston, 2015.

[2] Harris, S.: ALL IN ONE CISSP® EXAM GUIDE, Sixth Edition, McGraw-Hill Companies, New York, 2013.

[3] *Zakon o informacijskoj sigurnosti Republike Hrvatske,* lipanj 2017., http://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2484.html.

[4] URL: http://whatis.techtarget.com/definition/sensitive-information , (pristupljeno: travanj 2017.).

[5] URL: http://azop.hr/images/dokumenti/217/zastita_op_rh.pdf (pristupljeno: travanj 2017.),.

[6] North American Electric Reliability Corporation, Security Guideline for the Electricity Sector: Protecting Potentially Sensitive Information, Atlanta, 2012.

[7] Zakon o tajnosti podataka Republike Hrvatske, http://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2483.html (pristupljeno: svibanj 2017.).

[8] The International Council of E-Commerce Consultants: Penetration Testing: Procedures and Methodologies. Course Technology; 1 edition, 2010.

[9] URL: https://www.symantec.com/content/dam/symantec/docs/reports/2017-norton-wifi-risk-report-global-results-summary-en.pdf (pristupljeno prosinac 2017.).

[10] iPass Corporate Headquarters: 2017 Mobile Security Report , URL: https://www.ipass.com/wp-content/uploads/2017/05/iPass-2017-Mobile-Security-Report.pdf (Pristupljeno: Prosinac 2017.

[11] Globalni tim za istraživanje i analizu iz Kaspersky Laboratorija: The Darkhotel APT, a story of unusual hospitality, 2014..

[12] Korać M., Car D.: RADNI MATERIJAL – Uvod u računalne mreže, Visoko učilište Algebra, Zagreb, 2014..

[13] Datt, S.: Mrežna forenzika - zaštitita mreže od unutarnjih i vanjskih ugroza, hakera i zlonamjernog softvera [ekstrahirano iskustvo zajednice], Impresum, Dobar plan, Zagreb 2016..

[14] Engebretson, P.: The Basics of Hacking and Penetration Testing Ethical Hacking and Penetration Testing Made Easy, Second Edition, Elsevier, 2013..

[15] Justin Hutchens: Kali Linux Network Scanning Cookbook, Packt Publishing Ltd., Birmingham, 2014..

[16] URL: http://www.ieee.hr/_download/repository/LAN.pdf / (pristupljeno: lipanj 2017.).

[17] Ilyas, M., Ahson, S. A.: Handbook of Wireless Local Area Networks - Applications, Technology, Security, and Standards,, Taylor & Francis Group, Boca Raton, 2005.

[18] Eian, M., Mjølsnes, S. F.: A Formal Analysis of IEEE 802.11w Deadlock Vulnerabilities, Department of Telematics Norwegian University of Science and Technology (NTNU) Trondheim, Norveška, 2012.

[19] URL: https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c04498304 (pristupljeno: studeni 2017.).

[20] URL: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements (siječanj: 2018).

[21] URL: https://tools.ietf.org/html/rfc8110 (pristupljeno siječanj 2018.).

[22] URL: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-06-267.pdf (pristupljeno: lipanj 2017.).

[23] URL: https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf (pristupljeno studeni 2017.).

[24] Vanhoef, M., Piessens, F.: Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2, University of Leuven in Flanders, Belgija, 2017..

[25] Gan, D., Waliullah, M.: Wireless LAN Security Threats & Vulnerabilities,, International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1, 2014.

[26] Choi, Y. B., Muller, J., Kopek, C. V., i Makarsky J. M.: Corporate wireless LAN security - threats and an effective security assessment framework for wireless information assurance, International Journal of Mobile Communications, Vol. 4, No. 3, 2006..

[27] Xu, W., Grant, G., Nguyen, H., i Dai, X.: Security Breach - The Case of TJX Companies, Inc., Communications of the Association for Information Systems, 2008. .

[28] Dhiman D.: WLAN Security Issues and Solutions, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 1, Ver. IV (Jan. 2014), str. 67-75.

[29] URL: https://bib.irb.hr/datoteka/407502.Smaugos2ns2008_drvodericdiplomski_rad.pdf (pristupljeno: srpanj 2017.).

[30] URL: https://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf (pristupljeno: srpanj 2017.).

[31] URL: https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Wireless_Guidelines.pdf (Pristupljeno: studeni 2017.).

[32] Oriyano S-P.: CEH™ Certified Ethical Hacker Study Guide (Version 9), John Wiley & Sons, Inc., Indianapolis, 2016.

[33] URL: https://media.readthedocs.org/pdf/pentest-standard/latest/pentest-standard.pdf (pristupljeno: kolovoz 2017.).

[34] Gangan, S.; A Review of Man-in-the-Middle Attacks, New York, 2015..

[35] URL: https://ourcodeworld.com/articles/read/422/how-to-perform-a-man-in-the-middle-mitm-attack-with-kali-linux (pristupljeno: rujan 2017.).

[36] URL: https://www.networkmanagementsoftware.com/what-is-syslog/ (pristupljeno: travanj 2018.).

[37] URL: https://tools.ietf.org/html/rfc1035 (Pristupljeno: travanj 2018.).

[38] Abdelsalam, A. M., El-Sisi, A. B., Reddy, V. K., Mitigating ARP Spoofing Attacks in Software-Defined Networks, Faculty of Computers and Information, Menoufia University, Menoufia 2015., Egipat.

POPIS KRATICA

AES - *Advanced Encryption Standard*

AP - *access point*

ARP - *Address Resolution Protocol*

BSS - *Basic Service Set*

BSSID - BSS *Identifier*

CCMP - *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*

CLI - *Command-Line Interface/Interpreter*

CNSA - *Commercial National Security Algorithm*

DLL - *Data Link Layer*

DNS - *Domain Name System*

DNSSEC - *Domain Name System Security Extensions*

DoS - *Denial of service,*

EAP - *Extensible Authentication Protocol*

ESSID - ESS *Identifier*

FDDI - *Fiber Distributed Data Interface*

FTP - *File Transfer procotol*

GUI - *graphical user interface*

HTTP - *Hypertext Transfer procotol*

ICMP - *Internet Control Message Protocol*

IEEE - *Institute of Electrical and Electronics Engineers*

IK - informacijsko komunikacijski sustav

IPsec - Internet Protocol Security Protocol

ISO - *International Organization for Standardization*

IV - inicijalizacijski vektor

KRACK -*Key Reinstallation Attack*

LAN - *Local Area Connection*

LLC - *Logical Link Control*

MAC - *Media Access Control*

MITM - *Man-in-the-middle*

NAC - *Network Access Control*

NSE - *Nmap Scripting Engine*

OS - operativni sustav

OSI - *Open system interconnection*

OWE - *Opportunistic Wireless Encryption*

PBX - *Private Branch Exchange*

PCI DSS - *Payment Card Industry Data Security Standard*

PSK - *Pre-Shared Key*

RADIUS - *Remote Authentication Dial In User Service*

RF - radio frekvencijski

RSN - *Robust Security Network*

SMTP - *Simple Mail Transfer Protocol*

SSL - *Secure Sockets Layer*

TCP *Transmission Control Protocol*

TKIP - *Temporal Key Integrity Protocol*

TLS - *Transport Layer Security*

UDP - *User Datagram Protocol*

URL - *Uniform Resource Locator*

VPN - *Virtual private network*

WEP - *Wired Equivalent Privacy*

WIPS - *Wireless intrusion prevention system*

WLAN - *Wireless Local Area Network*

WPA - *Wi-Fi Protected Access*

WPS - *WiFi Protected Setup*

POPIS SLIKA I 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 Validacija sigurnosti bežične pristupne točke s ciljem sprječavanja pristupa osjetljivim informacijama na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

Student/ica:

U Zagrebu, 4/25/2018 _____

(potpis)