KAUNO KOLEGIJA

TECHNOLOGIJŲ FAKULTETAS

INFORMATIKOS IR MEDIJŲ TECHNOLOGIJŲ KATEDRA

Tautvydas Mikelionis

SIMULIACINĖ APLINKA DHCP PROTOKOLO ATAKŲ TYRIMAMS

Baigiamasis darbas

Kibernetinių sistemų ir saugos studijų programos
valstybinis kodas 6531BX024
Informatikos inžinerijos studijų krypties

Vadovas Paulius Baltrušaitis

Konsultantai dr. Jovita Danielytė

Gintarė Jurkševičiūtė

Kaunas, 2024

TURINYS

LENTELIŲ IR PAVEIKSLŲ SĄRAŠAS

LENTELĖS

PAVEIKSLAI

SĄVOKŲ SĄRAŠAS

Sąvoka	Aprašymas	Nuoroda į šaltinį
DDoS	Paskirstyta paslaugos trikdymo ataka – kibernetinė ataka, skirta informacinių sistemų užvaldymui, sutrukdyti vartotojų prisijungimui prie serverių	*(Qtar Labs,2023)*
DHCP Rogue Server	Ataka kuri įtraukia neteisėtą serverį į tinklą, kuris paskirsto klaidingus arba kenksmingus tinklo parametrus. Tai leidžia užpuolikui nukreipti arba perimti tinklo eismą, galimai išskleidžiant kenkėjiškas programas arba pavogiant konfidencialią informaciją.	*Undag, E (2019)*
DHCP	*DHCP* protokolas (Dinaminio kompiuterio konfigūravimo protokolas).	*Hero Wintolo, Yuliani Indrianingsih, Wahyu Hamdani, Syafrudin Abdie. (2023)*
DHCP Starvation	Ataka kuri neleidžia teisėtiems naudotojams gauti reikiamų tinklo konfigūracijų, sutrikdydama įprastą tinklo veikimą ir galimai sukeldama operacijų paralyžių.	*(Gihan, K. (2021) (Tamsir Ariyadi, Aidil NurRiyansyah, M. Agung, M. Alzi Ikrar 2023)*
GNS3	Tinklo modeliavimo įrankis, kuris leidžia simuliuoti realias tinklo aplinkas virtualioje aplinkoje.	*(„GNS3" dokumentacija)*
WireShark	tinklo analizės įrankis kuris leidžia perimti ir analizuoti tinklo srautą realiu laiku pateikdamas išsamią informaciją apie siunčiamus paketus.	*(„Wireshark" dokumentacija)*
Kali Linux	Tai specializuota operacinė sistema skirta IT saugumo specialistams atlikti tinklo saugumo patikrinimus, pažeidžiamumų analizę ir įsilaužimo testavimą.	*(„Kali Linux" dokumentacija)*
Yersinia	Pats įrankis yra skirtas įvairių tinklo protokolų saugumo testavimui ir atakoms. Jis naudojamas analizuoti ir išnaudoti pažeidžiamumus įvairiuose tinklo protokoluose.	*(„Yersinia" dokumentacija)*
TShark	*TShark* yra komandinės eilutės įrankis, naudojamas tinklo srauto analizavimui ir paketų gaudymui. Tai yra *WireShark* komandinės eilutės versija.	*(„TSark" dokumentacija)*

SANTRAUKA

Autorius Tautvydas Mikelionis. ***Simuliacinė aplinka DHCP protokolo atakų tyrimams.*** **Baigiamasis darbas. Vadovas Paulius Baltrušaitis. Kauno kolegija, Technologijų fakultetas, Informatikos ir medijų technologijų katedra. Kaunas, 2024, 54 psl.**

Reikšminiai žodžiai: *DHCP, DHCP Starvation, VMware, GNS3, DHCP Rogue Server, DHCP snooping.*

DHCP yra esminis tinklo protokolas, leidžiantis automatiškai priskirti IP adresus ir kitus tinklo parametrus įrenginiams, tačiau jis taip pat suteikia įvairias pažeidžiamybes, kurias gali išnaudoti kibernetiniai nusikaltėliai. Tyrimas, atliekamas naudojant *VMware* ir *GNS3*, susitelkia į dvi specifines *DHCP* protokolo atakas: *DHCP Starvation* ir *DHCP Rogue Server*. Šios atakos demonstruoja, kaip užpuolikai gali manipuliuoti tinklo resursais ir perimti duomenų srautą, sukeldami rimtų saugumo problemų. *DHCP Starvation ataka:* vykdoma siunčiant masines *DHCP* užklausas su suklastotais MAC adresais, siekiant išnaudoti visus serveryje esančius IP adresus. Tai neleidžia teisėtiems naudotojams gauti reikiamų tinklo konfigūracijų, sutrikdydama įprastą tinklo veikimą ir galimai sukeldama operacijų paralyžių. *DHCP Rogue Server ataka:* įtraukia neteisėtą serverį į tinklą, kuris paskirsto klaidingus arba kenksmingus tinklo parametrus. Tai leidžia užpuolikui nukreipti arba perimti tinklo eismą, galimai išskleidžiant kenkėjiškas programas arba pavogiant konfidencialią informaciją. Šios atakos yra ypač svarbios ir opios visuomenei, nes daugelis organizacijų ir įmonių priklauso nuo saugių ir stabilų tinklų veikimo. Nepakankamas dėmesys *DHCP* saugumui gali leisti užpuolikams lengvai patekti į korporatyvinius tinklus, kelti grėsmę duomenų saugumui ir netgi sukelti finansinius nuostolius. Tyrimo metu įgyvendintos simuliacijos ir atlikti testai suteikia vertingų įžvalgų, kaip galima stiprinti tinklo saugumą, pavyzdžiui, taikant *DHCP snooping*, MAC adresų filtravimą ar statinį IP priskyrimą. Tai padeda suformuoti geresnę apsaugos strategiją ir užtikrina, kad organizacijos galėtų efektyviai apsisaugoti nuo potencialių atakų. Tyrimas taip pat skatina viešą diskusiją apie tinklo saugumo svarbą ir būtinybę investuoti į atitinkamas technologijas bei žmogiškuosius išteklius, siekiant užtikrinti tinklo ir duomenų saugumą.

SUMMARY

Author Tautvydas Mikelionis. ***Simulation Environment for Investigating DHCP Protocol Attacks.*** **Graduation Thesis. Supervisor Paulius Baltrušaitis. Kauno kolegija HEI, Faculty of Technologies, Department of Informatics and Media Technology. Kaunas, 2024, 54 pages.**

Keywords: *DHCP, DHCP Starvation, VMware, GNS3, DHCP Rogue Server, FHCP snooping.*

DHCP is a fundamental network protocol that automatically assigns IP addresses and other network parameters to devices, but it also presents various vulnerabilities that can be exploited by cybercriminals. The research, conducted using *VMware* and *GNS3*, focuses on two specific *DHCP* protocol attacks: *DHCP Starvation* and *DHCP Rogue Server*. These attacks demonstrate how attackers can manipulate network resources and intercept data flow, causing serious security issues. *DHCP Starvation attack:* conducted by sending mass *DHCP* requests with forged MAC addresses, aiming to exhaust all available IP addresses in the server. This prevents legitimate users from obtaining necessary network configurations, disrupting normal network operation and potentially causing operational paralysis. *DHCP Rogue Server attack:* involves introducing an unauthorized server into the network, which distributes incorrect or malicious network parameters. This allows the attacker to redirect or take over network traffic, potentially deploying malware or stealing confidential information. These attacks are particularly significant and pressing for society because many organizations and companies depend on secure and stable network operations. Insufficient attention to *DHCP* security can allow attackers easy access into corporate networks, threatening data security and even causing financial losses. The simulations and tests implemented during the study provide valuable insights on how to strengthen network security, for example, through *DHCP snooping*, MAC address filtering, or static IP assignment. This helps form a better protection strategy and ensures that organizations can effectively safeguard against potential attacks. The research also encourages public discussion about the importance of network security and the need to invest in appropriate technologies and human resources to ensure the safety of networks and data.

ĮVADAS

Šiuolaikiniame pasaulyje, kai technologijos yra neatsiejama mūsų gyvenimo dalis, tinklo ir interneto saugumas tampa labai svarbiu faktoriumi ir reikšmingu klausimu visiems. Didėjantis interneto naudojimas, mobiliųjų įrenginių, kompiuterių, serverių bei įmonių skaičiaus augimas ir besiplečianti interneto infrastruktūra verčia imtis vis griežtesnių apsaugos priemonių panaudojimo, bei žinių įgijimo siekiant apsaugoti mūsų visų ar įmonės duomenis ir užtikrinti tinklo patikimumą. Tačiau kartu su technologinėmis pažangomis atsiranda ir naujos kibernetinės atakos, grėsmės ir iššūkiai, kurie kelia rimtą pavojų mūsų asmeninių duomenų ir tinklų saugumui. Nuo verslo komunikacijos iki kiekvieno iš mūsų asmeninių susirašinėjimų, beveik viskas šiandieną priklauso nuo interneto. Tai labai palengvina mūsų kasdienybę, suteikia daugiau laisvės ir ekonomiškumo dirbant, suteikia daugiau galimybių verslo spektre, tačiau tai reiškia, kad tinklo infrastruktūros sauga tampa esmine organizacijų, įmonių ir kiekvieno žmogaus prioritetu.

Kartu su technologinėmis pažangomis atsiranda ir naujos kibernetinės grėsmės ir jų padariniai bei iššūkiai, kurie kelia rimtą pavojų tinklo ir duomenų saugumui. Nuolat besivystantis kibernetinis karas ir jo kraštovaizdis reikalauja nuolatinio tobulėjimo ir įgyvendinimo saugumo priemonių, kurios būtų atsparios naujoms dar neregėtoms ir neatpažįstamoms atakoms ir pažeidžiamumams. Naujų technologijų diegimas sukelia nemažai iššūkių, nes jie dažnai remiasi *DHCP* protokolu ir taip kiekviena prijungta prietaisų grupė tampa potencialu taikiniu kibernetiniams įsilaužėliams.

Viena iš esminių kibernetinės saugos problemų yra susijusi su dinaminiu prievadų konfigūracijos protokolu (*DHCP*), kuris yra vienas iš pagrindinių tinklo valdymo įrankių, leidžiantis automatiškai priskirti IP adresus įvairiems tinklo įrenginiams. Nors pats *DHCP* suteikia didelį lankstumą ir efektyvumą tinklo administravime, taip pat jis gali tapti potencialiu taikiniu kibernetinių atakų rengėjams.

Šiai dienai remiantis statistikos duomenimis 2023m. galime matyti, kad antrąjį 2023 metų ketvirtį DDoS atakų vektorių pasiskirstyme yra daug pokyčių. Labiausiai pastebimas pokytis buvo UDP Flood atakų padidėjimas kuris išaugo nuo 37,44% iki 60,1% lyginant su pirmuoju ketvirčiu. SYN Flood patyrė padidėjima nuo 17,63% iki 18,1%.

Darbo problema – plečiantis tinklų infrastruktūrai ir atsirandant naujoms technologijoms kurios nuolat tobulėja, iškyla daug iššūkių ir grėsmių tokių kaip: didelis *DHCP* protokolų pažeidžiamumas, padidėjęs pavojus organizacijoms ir asmenims, naujos atakų formos ir metodai, didelis atakų mastas. Šiai dienai trūksta kibernetinių pažeidžiamumų duomenų, kad būtų galima pritaikyti mašininį mokymąsi efektyviam pažeidimų identifikavimui ir prevencijai.

Darbo objektas – simuliacinės aplinkos sukūrimas, *DHCP* protokolų atakos ir sauga

1. **Darbo tikslas –** simuliacinės aplinkos sukūrimas *DHCP* atakų duomenų generavimui ir analizei.

Darbo uždaviniai:

1. Apžvelgti *DHCP* protokolą ir jo funkcijas
2. Išanalizuoti *DHCP* atakų procesus ir naudojamas priemones. Ištirti pasekmes ir pavojus kylančius dėl atakų
3. Suprojektuoti simuliacinę platformą *DHCP* atakų simuliavimui ir duomenų srauto fiksavimui.
4. Platformą išbandyti atliekant *DHCP* atakų simuliacijas.
5. Įvertinti rezultatus ir pateikti išvadas bei rekomendacijas

Darbo metodai:

1. Mokslinės literatūros apžvalga, analizė ir apibendrinimas
2. Statistinė tyrimo duomenų analizė ir apibendrinimas

Bakalauro darbo pagrindinės dalies struktūra:

1. Apžvelgdami *DHCP* protokolų atakas bei rizikas kuo daugiau išanalizuojame ir ištiriame keletą atakų rūšių LAN tinkle.
2. Aprašomi ir pateikiami tyrimų rezultatai, pateikiamos rekomendacijos kaip išvengti atakų
3. Analizuojant atakas nustatyti kokios rizikos kyla asmenims bei įmonėms, nustatoma kaip galima kuo greičiau ir lengviau atakas identifikuoti

1. ANALITINĖ DALIS

1.1. *DHCP* protokolų apžvalga ir jo funkcijos

Dynamic Host Configuration Protocol (*DHCP*) yra tinklų protokolas, jis suteikia automatizavimą IP (Internet Protocol) priskyrime ir konfiguracijoje tinklo įrenginiams. *DHCP* turi keletą pagrindinių funkcijų kurias dabar apžvelgsime. (Tamsir Ariyadi, Aidil NurRiyansyah, M. Agung, M. Alzi Ikrar 2023):

IP adresų priskyrimas: *DHCP* yra nepakeičiamas įrankis tinklo administratoriams, leidžiantis efektyviai valdyti IP adresų priskyrimą įrenginiams. Jo veikimo principas grindžiamas dinamišku IP adresų suteikimu - kai įrenginys prisijungia prie tinklo, *DHCP* serveris automatiškai suteikia jam laisvą IP adresą iš prieinamo adresų diapazono. Tai palengvina administravimo procesą, kadangi nereikia rankiniu būdu konfigūruoti kiekvieno įrenginio IP adreso. Be to, *DHCP* taupo laiką ir išteklius, efektyviai pritaikydamas adresų suteikimą pagal tinklo poreikius. Svarbiausia, kad ši dinaminė priskyrimo sistema užtikrina, jog tinklo įrenginiai visada turės galiojančius IP adresus, o administratoriams nereikės nuolat stebėti ir tvarkyti adresų paskirstymo. Taigi, *DHCP* ne tik palengvina administravimą, bet ir padeda išlaikyti tinklo efektyvumą ir stabilumą.

IP konfigūracijos teikimas: *DHCP* neapsiriboja tik IP adresų priskyrimu, bet taip pat teikia įvairių kitų svarbių tinklo konfigūracijos parametrų. Be įrenginiams suteikiamų IP adresų, *DHCP* serveris taip pat pateikia kitus esminius tinklo parametrus, kurie būtini sklandžiam tinklo veikimui. Vienas iš svarbiausių teikiamų parametrų yra numatytasis maršrutų nustatymas. Tai leidžia nustatyti maršrutus, kuriuos įrenginiai turi naudoti, kad galėtų patekti į kitus tinklo segmentus arba pasiekti išorinį internetą. Be to, *DHCP* suteikia DNS serverių adresus, kurie būtini tinklo įrenginiams vertinant internetinius adresus į IP adresus ir atvirkščiai. Tai svarbu užtikrinti, kad tinklo įrenginiai galėtų teisingai interpretuoti interneto adresus ir tinkamai nukreipti duomenų srautą. Kitas svarbus teikiamas parametras yra *gateway* - tai tinklo įrenginys, per kurį įrenginiai gali patekti į išorinį tinklą, pvz., internetą. *DHCP* suteikia šio įrenginio adresą, leisdama įrenginiams patekti į išorinį tinklą ir bendrauti su kitais tinklo segmentais.

Be šių pagrindinių parametrų, *DHCP* taip pat gali teikti kitus tinklo nustatymus, tokius kaip laiko serverio adresą, *subnet mask* ir pan. Visa tai padeda optimizuoti tinklo veikimą ir leidžia tinklo administratoriams efektyviai valdyti ir konfigūruoti tinklo įrenginius. Taigi, *DHCP* ne tik suteikia IP adresus, bet ir užtikrina, kad tinklo įrenginiai būtų tinkamai sukonfigūruoti ir paruošti veikti tinklo aplinkoje.

IP adresų nuoma ir atnaujinimas: *DHCP* serveriai veikia pagal IP adresų nuomos modelį, kuris yra laikinis ir dinamiškas. Kai naujas įrenginys jungiasi prie tinklo, *DHCP* serveris suteikia jam laikiną IP adresą iš turimų adresų diapazono. Tačiau šis IP adresas yra skirtas tik tam tikram laikui, nustatytam *DHCP* serverio konfigūracijoje. Kai šis laikas pasibaigia arba klientas atsijungia nuo tinklo, IP adresas tampa laisvas ir grąžinamas į adresų pool'ą, kad būtų panaudotas naujiems klientams. Šis dinamiškas adresų priskyrimo modelis leidžia efektyviai valdyti turimus IP adresus, užtikrinant, kad jie būtų naudojami tik tada, kai reikia, ir kad tinklas būtų lankstus bei efektyvus. Taip pat tai padeda išvengti adresų konfliktų ir nereikalingo resursų švaistymo, palengvindamas tinklo administravimą.

Automatinis konfigūracijos atnaujinimas: *DHCP* pasižymi automatišku konfigūracijos atnaujinimu. Kai pasikeičia tinklo parametrai arba klientui priskiriamas naujas IP, *DHCP* automatiškai atnaujina kliento įrenginio konfigūraciją. Tai užtikrina, kad visi tinklo įrenginiai visada turės tinkamą konfigūraciją, atitinkančią naujausius tinklo nustatymus ir reikalavimus. Automatinis atnaujinimas palengvina tinklo administravimą, nes nereikia rankiniu būdu konfigūruoti kiekvieno įrenginio atskirai. Taip pat tai padeda išvengti konfigūracijos nesuderinamumo ir užtikrina, kad visi tinklo įrenginiai veiktų optimaliai ir saugiai.

Centralizuota administravimo galimybė: *DHCP* suteikia galimybę centralizuotai valdyti visus turimus IP adresus ir konfigūracijos parametrus. Tai reiškia, kad administravimas vyksta iš vienos vietos - *DHCP* serverio, kuriame yra saugomi visi tinklo nustatymai. Administravimas centralizuotai leidžia efektyviai ir lengvai valdyti visus IP adresus, nustatymus ir parametrus, taip palengvinant tinklo priežiūrą ir administravimą. Be to, tai užtikrina, kad visi tinklo įrenginiai naudoja vienodus nustatymus, konsistentišką konfigūraciją ir užtikrina tinklo stabilumą bei saugumą.

Didinamas tinklo efektyvumas: *DHCP* automatinis IP adresų priskyrimas suteikia didelį pranašumą dideliuose tinkluose. Jis leidžia efektyviai tvarkyti didelius įrenginių kiekius, nereikalaujant rankinio kiekvieno įrenginio konfigūravimo. Dėl automatinio priskyrimo administravimas tampa efektyvesnis, taupydamas laiką ir resursus. Tai leidžia didelių įmonių administratoriams lengvai valdyti ir priežiūrėti platų įrenginių parką, kartu užtikrinant, kad visi įrenginiai gautų tinkamus tinklo nustatymus ir būtų pasirengę veikti tinklo aplinkoje. Automatizavimas taip pat sumažina galimų klaidų riziką, užtikrinant tinklo efektyvumą ir patikimumą. Išnagrinėti pagrindinius *DHCP* atakų tipus ir poveikį saugumui

Kaip ir kiekvienas geras išradimas ar įvykis taip ir *DHCP* turi savų minusų. *DHCP* yra labai jautrus tinklo protokolas, kuris yra pažeidžiamas įvairiomis atakomis. Štai keletas pagrindinių atakų tipų ir jų poveikis saugumui.

***DHCP* įsilaužimas (*DHCP Spoofing*):** *DHCP* įsilaužimas (*DHCP Spoofing*) yra kai įsilaužėlis apsimeta esąs *DHCP* serveris ir siunčia klaidingus IP adresus bei konfigūracijos

parametrus klientams. Ši ataka leidžia įsilaužėliui nukreipti klientų srautą per savo sukurtą tinklą ir gali padaryti didelę žalą. Jei ataka pavyksta, įsilaužėlis gali pasisavinti jautrius duomenis, prisijungimus ir netgi užgrobti klientų srautą. Tai kelia rimtą grėsmę tinklo saugumui ir gali sukelti žalos reputacijai, duomenų praradimui ar net teisiniams padariniams. Šiai atakai įveikti būtina imtis tinkamų saugumo priemonių, tokių kaip *DHCP snooping* (Dio Aditya Pradana, Ade Surya Budiman, 2020.), MAC filtravimas ar tinklo apsaugos įrankių naudojimas.

***DHCP* atakos, prarandant nuomos informaciją (angl. *DHCP* Lease Exhaustion):** yra vienas iš būdų, kaip kibernetiniai nusikaltėliai gali sutrikdyti tinklo veikimą. Ši ataka yra vykdoma kūrus savo, klastotą *DHCP* serverį, kuris aktyviai siunčia didelį kiekį *DHCP* užklausų tikrais ar suklastotais MAC adresais. Tai daroma siekiant išnaudoti tikrojo, teisėto *DHCP* serverio IP adresų fondą. Kai realus *DHCP* serveris išnaudoja visus galimus IP adresus, nauji ar atnaujinantys savo IP klientai negali gauti IP adresų nuomų. Tai lemia, kad įrenginiai nebegali prisijungti prie tinklo ir dalyvauti įprastoje tinklo veikloje. Taip klientų įrenginiai tampa nepasiekiami ar riboja jų gebėjimą naudotis tinklo resursais.

***DHCP* serverio užkrova (SHCP Server Overload):** kibernetinės atakos forma, kurioje įsilaužėlis kuria dirbtinai didelį netikrų klientų skaičių, siekdamas apkrauti *DHCP* serverį. Įsilaužėliai masiškai generuoja *DHCP* užklausas naudodami suklastotus arba atsitiktinai sugeneruotus MAC adresus. Šis veiksmas sukuria itin didelę apkrovą serveriui, kadangi jis bando apdoroti kiekvieną užklausą, skirdamas IP adresus, kas išnaudoja jo procesorius ir atmintį, dėl ko serveris gali pradėti veikti netinkamai ar net visiškai sustoti. Tokios atakos metu tinklo administratoriai gali būti priversti atstatyti serverio veiklą, o tai suteikia įsilaužėliams galimybę nesunkiai patekti į kitus serverio resursus ar net pačią infrastruktūrą. Atakos metu gali būti praleisti svarbūs saugumo įspėjimai, kadangi dėmesys yra nukreiptas į akivaizdžius veiklos sutrikimus. Tai sudaro palankias sąlygas įsilaužėliams vykdyti kitas kenkėjiškas operacijas, nes sistemų saugumo stebėjimas ir reakcija į įvykius gali būti susilpnėję.

Man in the Middle (MitM) atakos: Man in the Middle (MitM) atakos yra vienas iš pažangesnių kibernetinio įsibrovimo metodų, kai įsilaužėlis įsiterpia tarp kliento ir tikrojo *DHCP* serverio. Šiame scenarijuje įsilaužėlis kuria dirbtinį ryšį, kad perimtų ir kontroliuotų visą duomenų srautą tarp šių dviejų šaltinių. Sukūręs šį tarpinį ryšį, įsilaužėlis gali ne tik stebėti ir registruoti visus siunčiamus ir gaunamus pranešimus, bet ir juos keisti bei filtruoti, prieš perduodant toliau. Dėl šios atakos įsilaužėlis gali įgyti prieigą prie konfidencialios informacijos, įskaitant slaptažodžius, finansinius duomenis ir asmens duomenis. Be to, *MitM* atakos leidžia įsilaužėliui manipuliuoti komunikacija, pavyzdžiui, keisti maršrutizacijos informaciją ar netgi siųsti kenkėjiškas programines įrangas ir atnaujinimus.

***DHCP* serverio apkrovimas (*DHCP* Server Flooding):** kibernetinės atakos metodas, kurį naudojant įsilaužėlis bando perkrauti *DHCP* serverį siųsdamas didžiulį kiekį netikrų ar klaidingų *DHCP* užklausų. Šis metodas siekia sunaikinti serverio gebėjimą efektyviai aptarnauti tinklo įrenginius, nes serveris užsiėmęs tvarkydamasis su netikromis užklausomis ir dėl to negali teikti IP adresų teisėtiems klientams. Perkrovus *DHCP* serverį, viso tinklo veikimas gali būti sutrikdytas, nes tinklo įrenginiai (pvz., kompiuteriai, mobiliųjų telefonų, planšetiniai kompiuteriai) negali gauti ar atnaujinti savo IP adresų, o tai veda prie jų atsijungimo nuo tinklo ar ryšio kokybės pablogėjimo. Be to, kai serveris yra užimtas tvarkantis su klaidingomis užklausomis, tai suteikia įsilaužėliams galimybes panaudoti kitas sudėtingesnes atakos formas, pvz., man-in-the-middle atakas ar net sukurti klastotinus *DHCP* serverius, kad nukreiptų eismą per jų kontroliuojamas sistemas.

***DHCP Starvation* (Gihan, K. 2021):** tai ataka, kai agresyvus kliento (arba įrenginio) įrankis prisiima daugybę *DHCP* adresų iš serverio. Jis siunčia daugybę *DHCP* užklausų, siekdamas išnaudoti visus ar didžiąją dalį *DHCP* adresų, paliekant kitus klientus be tinklo ryšio. Ši ataka persidengia su (*spoofing*) atakomis, kai kiti klientai negali gauti galiojančių IP adresų.

***DHCP Rogue Server*:** tai ataka, kurioje asmuo ar įrenginys veikia kaip neteisėtas *DHCP* serveris tinkle. Jis skleidžia netinkamus *DHCP* adresus klientams, kurie tada gali būti nukreipti į kenksmingus arba netinkamus tinklo ryšio taškus. Tai leidžia užpuolikui stebėti, keisti ar netgi užkariauti klientų duomenis.

1.2. *DHCP* atakų simuliavimui naudojamų įrankių apžvalga

***GNS3* (*GNS3. n.d.*) –** yra puikus tinklo modeliavimo įrankis, kuris leidžia simuliuoti realias tinklo aplinkas virtualioje aplinkoje. Tai atviro kodo programa, kuri leidžia kurti ir testuoti įvairias tinklo konfigūracijas, įtraukiant įvairius maršrutizatorius, komutatorius, serverius, virtualias mašinas ir kita.

***VMware (VMware n.d.)* –** yra puiki virtualizacijos programa, kuri leidžia kurti virtualias mašinas viename fiziniame kompiuteryje. *VMware* galima susieti su GN3 platforma ir taip sukurti virtualų tinklą kuriame yra prijungtos virtualios mašinos. Tai yra labai tinkama platforma norint testuoti *DHCP* atakas.

***Yersinia* –** tai įrankis kuris yra įtrauktas į *Kali Linux* specializuota operacinę sistemą kuri skirta saugumo specialistams. Pats įrankis yra skirtas įvairių tinklo protokolų saugumo testavimui ir atakoms. Jis naudojamas analizuoti ir išnaudoti pažeidžiamumus įvairiuose tinklo protokoluose.

***Kali Linux (Kali Linux n.d.)* –** tai specializuota operacinė sistema skirta IT saugumo specialistams atlikti tinklo saugumo patikrinimus, pažeidžiamumų analizę ir įsilaužimo testavimą. *Kali Linux* yra debian pagrindu sukurta operacinė sistema.

***WireShark* (*WireShark n.d.)*–** tinklo analizės įrankis kuris leidžia perimti ir analizuoti tinklo srautą realiu laiku pateikdamas išsamią informaciją apie siunčiamus paketus. Šis įrankis leidžia stebėti visus paketus kurie keliauja per tinklą ir daryti tinklo analizę.

1.3. Mašininio mokymosi metodai/algoritmai taikomi pažeidimams identifikuoti.

Yra daugybė mašinų galinčių aptikti atakas kelios iš jų tai SVM, ANN ir KNN. (Yildiran Yilmaz, Selim Buyrukoglu, 2023).

Support Vector Machine – yra gana populiarus algoritmas pažeidimams identifikuoti, jis mokomas naudojant surinktus duomenis iš turimų pažeidimų bei gali būti naudojamas klasifikuojant naujiems duomenims nurodant kaip pažeidimus arba ne

Artificial Neural Networks – kaip ir SVM ši dirbtinių tinklų mašina naudojama pažeidimams identifikuoti, mokant ją su turimais duomenimis.

K-Nearest Neighbors – tai paprastas algoritmas, kuris remiasi kaimynų principu ir taikomas pažeidimams identifikuoti pagal duomenų panašumus

WireShark – *WireShark* yra populiari tinklo analizės įrankis, leidžiantis stebėti ir analizuoti tinklo paketus. Jį galima naudoti siekiant stebėti *DHCP* užklausas ir atsakymus, taip identifikuojant potencialias atakas ir neįprastas veiklas.

Snort – Snort yra atviro kodo tinklo instrukavimų aptikimo sistema (IDS), kuri gali būti konfigūruojama aptikti ir reaguoti į įvairias tinklo pažeidimo formas, įskaitant *DHCP* atakas.

Norint kuo efektyviau naudotis mašininio mokymosi metodais ar algoritmais reikia atkreipti dėmesį į pažeidžiamų duomenų rinkimą ir jų transformavimą mašinoms, pagrindiniai aspektai būtų šie:

Duomenų rinkimas – būtina rinkti duomenis kurie apima tiek normalią tiek ir pažeistą ar pažeidžiamą tinklo veiklą.

Duomenų transformavimas – reikia atkreipti dėmesį į pačią mašiną su kuria dirbame ir kokie duomenys gali būti naudingi mokymuisi ir algoritmams. Pavyzdžiui, iš IP paketų galima išgryninti tam tikrus laukus, tokius kaip IP adresas, siuntėjo/gavėjo portai, paketo dydis ir pan.

Duomenų normalizavimas – Prieš pradedant mokymą svarbu normalizuoti duomenis, kad jie būtų panašaus masto.

Duomenų padalinimas – duomenis reikia padalinti į mokymo ir testavimo rinkinius.

1.4. Rekomendacijos, kaip stiprinti saugumą atsižvelgiant į DHCP spragas.

DHCP protokolas turi įvairių saugumo grėsmių, įskaitant aukščiau išvardintas atakas. Štai keletas rekomendacijų, kaip galime padidinti saugumą atsižvelgiant į *DHCP* spragas.

Naudokite statinį IP priskyrimą – Naudoti statinį IP priskyrimą yra puikus pasirinkimas mažose tinklo aplinkose, kur kompiuterių ar prietaisų skaičius yra nedidelis. Ši metodika reiškia, kad kiekvienam įrenginiui yra rankiniu būdu priskiriamas fiksuotas IP adresas, vengiant *DHCP* serverio naudojimo. Statinio IP priskyrimas sumažina riziką susidurti su įvairiomis *DHCP* protokolo saugumo grėsmėmis, įskaitant *DHCP* serverio perkrovimą, Man in the Middle ir Lease Exhaustion atakas, kadangi IP adresų priskyrimas nebevyksta dinamiškai per tinklo ryšį. Statinis IP priskyrimas taip pat leidžia griežčiau kontroliuoti tinklo konfigūraciją, užtikrinant, kad kiekvienas įrenginys visada turėtų tą pačią IP adresą, kas palengvina tinklo stebėjimą, nustatymų valdymą ir saugumo trikčių šalinimą. Be to, tai padeda išvengti IP konfliktų, kurie gali kilti naudojant *DHCP*, ypač esant klaidoms serverio konfigūracijoje.

Įdiekite *DHCP* filtravimą – Įdiegiant *DHCP* filtravimą, galima žymiai padidinti tinklo saugumą, nustatant filtrus, kurie leidžia aptikti ir blokuoti *DHCP* užklausas pagal nustatytus MAC adresus. Šis metodas leidžia administratoriui kontroliuoti, kurie įrenginiai gali gauti IP adresus iš *DHCP* serverio, apribojant galimybę neautorizuotiems ar potencialiai kenksmingiems įrenginiams prisijungti prie tinklo.

MAC adresų filtravimas veikia kaip pirmasis saugumo sluoksnis, nes leidžia serveriui aptarnauti tik iš anksto patvirtintus įrenginius. Tai yra ypač naudinga organizacijoms, kurios nori užtikrinti, kad tik patikimi įrenginiai būtų prijungti prie jų tinklų, sumažinant galimybę kenksmingiems įsilaužėliams arba suklastotoms įrangoms patekti į sistemą ir vykdyti atakas.

***DHCP snooping* –** *DHCP snooping* (Nuhu Abdulhafiz A., Echobu Faith O. and Olanrewaju Oyenike M 2020). yra saugumo funkcija, dažnai integruojama į išmaniuosius jungiklius ir maršrutizatorius, kuri skirta stebėti ir filtruoti *DHCP* srautus tinkle. Ši funkcija suteikia galimybę identifikuoti ir atskirti patikimus *DHCP* serverius nuo nepatikimų, veikdama kaip kontrolinis punktas prieš leidžiant *DHCP* atsakymams pasiekti klientų įrenginius. Įgyvendinant *DHCP snooping*, įrenginiai, kurie priskiriami kaip patikimi, gali siųsti *DHCP* atsakymus, o tie, kurie yra nepažymėti kaip patikimi, negali. Tai apsaugo nuo *DHCP* serverio klonavimo atakų, kuriose įsilaužėliai įveda suklastota *DHCP* serverį į tinklą su tikslu manipuliuoti ar pavogti duomenis iš tinklo klientų.

Dinaminis *VLAN* priskyrimas – išplėstinė tinklo valdymo funkcija, leidžianti automatiškai priskirti tinklo įrenginius į atitinkamas *VLAN* grupes remiantis jų MAC adresais. Ši funkcija padeda užtikrinti, kad įrenginiai būtų prijungti prie tinklo segmentų, kurie atitinka jų vartojimo profilį ar

saugumo reikalavimus, taip sumažinant netinkamo naudojimo ir nepageidaujamų įrenginių prisijungimo riziką.

Kai įrenginys pirmą kartą prisijungia prie tinklo, dinaminis *VLAN* priskyrimas analizuoja įrenginio MAC adresą ir, remiantis iš anksto nustatytais saugumo politikos kriterijais, priskiria įrenginį prie konkretaus *VLAN*. Toks metodas leidžia tinklą efektyviai segmentuoti, suteikiant skirtingus prieigos lygius pagal įrenginio paskirtį ar vartotojo grupę, užtikrinant aukštesnį duomenų konfidencialumo ir tinklo resursų prieinamumo lygį.

Sistemų atnaujinimas – Atnaujinant įrenginius reguliariai, galima užtikrinti, kad bus įdiegtos naujausios saugumo priemonės ir kad įrenginiai bus atsparūs naujausiems kibernetiniams iššūkiams. Tai apima ne tik saugumo pleistrus, bet ir programinės įrangos atnaujinimus, kurie gali pagerinti sistemos veikimą ir funkcionalumą, pavyzdžiui, pagerinant tinklo veikimo efektyvumą ar prieinamumą. Be to, sistemų atnaujinimas leidžia įmonėms laikytis teisinių ir reguliavimo reikalavimų, ypač susijusių su duomenų apsauga ir privatumu. Tai svarbu įmonėms, siekiant išvengti baudų už nesilaikymą saugumo standartų ir užtikrinti, kad jų veikla atitinka pramonės nustatytas gaires.

Monitoringas – yra gyvybiškai svarbus tinklo valdymo aspektas, ypač siekiant aptikti ir reaguoti į neįprastas *DHCP* užklausas bei kitus saugumo pažeidimus. Efektyvi tinklo stebėsena leidžia IT specialistams laiku identifikuoti ir spręsti potencialius incidentus, prieš juos tapus rimtesnėmis grėsmėmis. Tinklo monitoringo procesas apima eismo analizę realiuoju laiku, siekiant stebėti visus tinklo srautus ir aptikti bet kokius nukrypimus nuo įprastos veiklos. Tai apima didelio srauto užklausų, kurios gali rodyti *DHCP* serverio perkrovimo mėginimą, ar neįprastų MAC adresų, rodančių galimą klastočių *DHCP* serverių naudojimą, stebėjimą. Siekiant užtikrinti efektyvų monitoringą, organizacijos turėtų naudoti pažangius tinklo stebėjimo įrankius ir sistemas, pavyzdžiui, SIEM sistemas, kurios ne tik registruoja ir analizuoja duomenis, bet ir sukuria įspėjimus dėl potencialių saugumo incidentų. Šie įrankiai gali automatiškai pranešti apie įtartinus veiksmus ir padėti IT komandoms greitai reaguoti, minimizuojant galimą žalą.

1.5. Apibendrinimas

Dinaminis prievado konfigūravimo protokolas *(DHCP)* yra svarbus tinklo komponentas, kuris didina tinklo efektyvumą, suteikdamas galimybę automatiškai skirti ir konfigūruoti IP adresus tinklo įrenginiams. Šis protokolas leidžia tinklo administratoriams lengvai valdyti IP adresų paskirstymą, sumažina rankinio darbo kiekį ir padeda išvengti IP adresų konfliktų. Tačiau, nepaisant jo naudingumo, *DHCP* yra pažeidžiamas įvairioms kibernetinėms atakoms, kurios gali kelti rimtą grėsmę tinklo saugumui ir veikimui. Viena iš tokių atakų yra *DHCP Starvation*, kurioje užpuolikas

siunčia daugybę *DHCP* užklausų su skirtingais *MAC* adresais, siekdamas išnaudoti visus *DHCP* serverio IP adresus, taip sutrikdydamas teisėtų vartotojų prisijungimą prie tinklo. Kita rimta grėsmė yra *DDoS* ir *DoS* atakos, kuriose serveris užtvindomas užklausomis, sukeliantys serverio perkrovimą ir tinklo paslaugų sutrikdymą.

Be to, *DHCP* yra pažeidžiamas *Man-in-the-Middle (MitM)* atakoms, kuriose užpuolikas įsiterpia tarp *DHCP* kliento ir serverio, siekdamas perimti arba pakeisti perduodamus duomenis. Tai gali lemti neteisėtą duomenų perėmimą ir pavogimą. Kiti pavojai apima serverio perkrovimą, duomenų vagystę ir įvairias kitas kibernetines grėsmes, kurios gali sutrikdyti tinklo veiklą ir pažeisti duomenų saugumą.

Siekiant sumažinti šias pažeidžiamybes ir apsaugoti tinklą nuo galimų atakų, rekomenduojama įgyvendinti kelias saugumo priemones. Pirmiausia, būtina naudoti *DHCP snooping* technologiją, kuri padeda nustatyti ir blokuoti neteisėtas *DHCP* užklausas. Antra, tinklo segmentacija gali padėti sumažinti atakos paviršių, apribojant *DHCP* serverio veikimą tik tam tikruose tinklo segmentuose. Trečia, reikėtų reguliariai atnaujinti tinklo įrangą ir naudoti stiprias autentifikavimo priemones, tokias kaip 802.1X, kurios padeda užtikrinti, kad tik autorizuoti įrenginiai gali prisijungti prie tinklo. Galiausiai, svarbu nuolat stebėti tinklo veiklą, kad būtų galima anksti aptikti ir reaguoti į galimus saugumo incidentus. Įdiegus šias priemones, galima ženkliai padidinti *DHCP* protokolo saugumą ir sumažinti kibernetinių atakų riziką.

2. PROJEKTAVIMAS

2.1. Projektuojamo objekto paskirtis

Šio objekto paskirtis - ištirti atakas prieš *DHCP* protokolą ir pateikti saugumo priemones. Tai apima įvairių *DHCP* protokolo atakų apžvalgą ir analizę, jų poveikį tinklo saugumui ir priešpriešines priemones, siūlomas *DHCP* saugumui padidinti. Projekto tikslas - suprasti dabartines grėsmes *DHCP* protokolo naudojimui ir parengti rekomendacijas bei gaires, kaip nuo jų apsisaugoti.

2.2. Projektuojamo objekto funkcijos

Išnagrinėti *DHCP* protokolo veikimo principus ir pateikti pagrindines atakų rūšis. Padaryti tinklo topologijas *GNS3* platformoje ir ištestuoti kartu su virtualiomis mašinomis. Aptikti potencialas spragas tinklo saugumui ir pagrindinius pažeidžiamumus bei pateikti rekomendacijas ir saugumo prevencija prieš atakas.

2.3. Reikalavimai projektuojamo objekto posistemėms

3.2.1. Programiniai reikalavimai

Programiniai reikalavimai *DHCP* protokolų atakoms ir saugai nustatyti prasideda nuo pačios platformos kurioje rengiama tinklo topologija t.y *GNS3*. Reikalingos virtualios mašinos kurios sukuriamos su programa *VMware*. Reikalingi atakų rengimo įrankiai ir pačios atakų programos , tam naudojamas *Kali Linux* ir jame esančios programos pvz. *Yersinia, Ettercap* ir t.t. Duomenims rinkti reikalingos programos, šiam darbui buvo naudojama *WireShark* ir *TShark*. Reikalingi vartotojų kompiuteriai pvz. *Windows 10* aplinka.

3.2.2. Reikalavimai naudotojo sąsajai

Teikiama vartotojo sąsaja turi būti patogi, lengvai suprantama, greitai reaguojanti, kad įvairiems naudotojams būtų suteikiama maloni naudojimo patirtis, o į tai turi įeiti: sklandus naršymas, aiškūs darbo vietų sąrašai bei aktualūs filtrai.

3.2.3. Reikalavimai realizacijai

Vartotojo sąsaja turi atitikti aplinka kurioje būtų galimybė atlikti atakas bei jas analizuoti, šiuo atveju naudojama *Kali Linux* aplinka kuri yra patogi naudoti bei turi daug reikiamų programų kurių nereikia diegti pačiam. Tai pat reikalinga aplinka tinklo realizacijai, naudojama *GNS3* įskiepis. Reikalingos kelios virtualios mašinos. Būtinas interneto ryšys.

3.2.4. Reikalavimai eksploatavimui

Eksploatavimui reikalingas tinkamas įrangos ir programinės įrangos rinkinys, siekiant užtikrinti efektyvų ir saugų tinklo veikimą. Tarp šių priemonių yra būtinas interneto ryšys, tinklo srauto stebėjimo priemonės, tinklo sudarymo įrankiai ir virtualios mašinos aplinka.

3.2.5. Reikalavimai saugumui

Svarbu, kad viskas turi veikti vietiniam tinkle, atakos atliekamos nepažeidžiant konkrečių ir realių svetainių ar vartotojų kompiuterių. Tai reiškia, kad nenaudojami jokie konkretūs serveriai ir realios svetainės, siekiant užtikrinti privatumo politikos laikymąsi ir apsaugoti tikrus vartotojus nuo galimų pavojų.

3. PROJEKTINĖ DALIS

3.1. Sistemos architektūra

Architektūra sukurta naudojant *GNS3* platformą ir *VMware,* tai yra puikūs įrankiai mokymosi ir eksperimentavimo aplinkai kurti. *GNS3* platforma yra naudojama virtualių tinklų kūrimui ir simuliacijai, leidžianti vartotojams modeliuoti įvairias tinklo topologijas ir konfigūruoti tinklo įrenginius pagal konkretų poreikį. Šis funkcionalumas suteikia galimybę išsamiai testuoti *DHCP* protokolo elgesį įvairiose situacijose, įskaitant atakų simuliacijas. *VMware,* naudojamas virtualizuoti serveriams ir kompiuteriams, leidžia sukurti realistinę ir kontroliuojamą kibernetinių žvalgybos operacijų aplinką. Šios virtualios mašinos gali būti konfigūruotos atlikti specifinius uždavinius, pavyzdžiui, imituoti *DHCP* serverio atakas, įskaitant *DHCP* "*starvation*" (išnaudojimą) ar "*spoofing*" (apgaulingą identifikavimą). Tai svarbu, nes galima įvertinti, kaip realūs tinklo įrenginiai ir saugumo sprendimai reaguoja į šiuos scenarijus. Projekto kritinis integracijos taškas užtikrina efektyvų duomenų mainus tarp *GNS3* ir *VMware* aplinkų, leidžiantis naudoti *GNS3* modeliuotus tinklus kaip testavimo platformą, o *VMware* mašinas – kaip atakų šaltinius ar taikinius. Tai yra būtina, norint išbandyti įvairias apsaugos priemones prieš *DHCP* atakas, įskaitant *DHCP snooping,* IP-MAC priskyrimo strategijas, ir atnaujinimus, kurie padeda sumažinti tinklo pažeidžiamumą.

Tokia architektūra yra idealiai tinka atlikti išsamius saugumo testus, modeliuojant realias kibernetinio saugumo grėsmes, taip suteikiant vertingų įžvalgų, kaip geriausiai apsaugoti tinklą nuo *DHCP* susijusių atakų. Sistemos architektūros funkcijos:

1. *GNS3* ir *VMware* integracija - *GNS3* naudota simuliuojant tinklo įrenginius ir jų sąveiką o *VMware* skirta virtualizuoti serverius ir jų kompiuterius.
2. Tinklo modeliavimo aplinka – *GNS3* suteikė aplinką, kurioje galima lengvai kurti ir konfigūruoti, keičiant topologijos išdėstymą, bei keičiant įrenginių nustatymus ir kt. Šios aplinkos dėka lengvai atlikta *DHCP* atakos ir aptiktos silpnos įrenginių vietos.
3. Virtualios mašinos *VMware* aplinkoje – *VMware* platforma skirta kurti ir valdyti virtualias mašinas, susidiegti norimas operacines sistemas, kurios atitiko poreikius. Šios virtualios mašinos naudojamos kaip pagrindinės sistemos dalys, kurių pagalba atlikta *DHCP* protokolo atakos bei stebėjimas.
4. Integracijos taškai – šie taškai reikalingi tam, kad *GNS3* sukurti tinklo modeliai galėtų lengvai bendrauti su *VMware* virtualiomis mašinomis.

3.2. Simuliuojamos tinklo topologijos sukūrimas

Sukurta tinklo topologija kuri lengvai simuliuojama ir konfigūruojama pagal reikiamus reikalavimus *DHCP* protokolo atakoms atlikti. Tinklas naudotas atlikti įvairioms *DHCP* protokolo atakoms atlikti bei stebėti duomenų srautą ir pažeidžiamumus. Tai esminis žingsnis leidžiantis atlikti išsamesnę atakų analizę ir testavimą.

3.2.1. Tinklo modelių kūrimas *GNS3* aplinkoje

Naudojant *GNS3* atviro kodo programa buvo sukurta tinklo topologija leidžianti atlikti kibernetines atakas. Topologija sudarė atakuojantis kompiuteris su *Kali Linux* sistema, vartotojo kompiuteris su *Windows 10* operacine sistema, komutatorius bei maršrutizatorius. Kiekvienas įrenginys atitinkamai sukonfigūruotas jog būtų galimybė atlikti atakas.

3.2.2. Virtualių mašinų kūrimas *VMware* aplinkoje

VMware aplinkoje sukurtos virtualios mašinos kurios vėliau susiejamos su *GNS3*. Viena iš mašinų su *Kali Linux* operacine sistema, kita su *Windows 10*. Kali Linux operacinė sistema yra svarbi, nes joje yra daug programų kurios naudojamos atakoms atlikti ir jų nereikia diegti papildomai tokių kaip *WireShark, Nmap, Ettercap*. *Windows 10* operacinė sistema yra plačiai naudojama paprastų vartotojų realiame tinkle, todėl yra pravartu analizuoti pažeidžiamumus ir stebėti kompiuterio veiklą kuris yra plačiai naudojamas. Pačias mašinas lengva valdyti ir konfigūruoti pagal reikiamus aspektus. Be šių sistemų atakų atlikimas ir virtualizacija būtų labai sudėtinga.

3.2.3. Integracija su *GNS3* ir *VMware*

Integracija tarp *GNS3* ir *VMware* yra būtina vykdant kompleksinius kibernetinius saugumo testus, ypač susijusius su *DHCP* atakų simuliacijomis. *GNS3* yra naudojama virtualių tinklų kūrimui, kurie leidžia modeliuoti realistiškas tinklo situacijas, įskaitant *DHCP* serverių ir klientų sąveiką. *VMware*, iš kitos pusės, suteikia galimybę virtualizuoti serverius ir darbo stotis, kurios gali būti naudojamos kaip atakos šaltiniai arba taikiniai. Integravus šias dvi platformas, galima sukurti labai dinamišką aplinką, kurioje įmanoma tiksliai stebėti ir analizuoti *DHCP* protokolo elgseną bei jo pažeidžiamumus. Pavyzdžiui, galima simuliuoti *DHCP* "*Starvation*" ataką, kurioje įsilaužėlis išnaudoja visus turimus IP adresus, arba "*spoofing*" ataką, kurioje naudojami suklastoti serveriai, siekiant nukreipti eismą per kenkėjišką įrangą. Siekiant šios integracijos, būtina užtikrinti, kad *GNS3*

ir *VMware* komponentai būtų tinkamai sukonfigūruoti ir kad tarp jų būtų efektyvus duomenų mainų kanalas. Tai reiškia, kad reikia atidžiai nustatyti tinklo adapterius ir kitus tinklo parametrus, kad būtų užtikrintas sklandus ir saugus ryšys tarp virtualių mašinų ir virtualių tinklų. Toks metodas leidžia ne tik identifikuoti ir analizuoti galimas grėsmes, bet ir vertinti skirtingas saugumo priemones, pavyzdžiui, *DHCP snooping*, filtravimą ir kitas strategijas, kurios padeda apsaugoti tinklą nuo neigiamo įsilaužėlių poveikio. Taip pat ši integracija padeda mokymosi ir tyrimų procese, teikdama praktinę patirtį ir giluminius tinklo saugumo įžvalgas.

3.2.4. Apibendrinimas

Viską apibendrinant, sukurta tinklo topologija naudojant *GNS3* atviro kodo programą, tai pat sukurtos virtualios mašinos su *Kali Linux* ir *Windows 10* operacinėmis sistemomis pasinaudojus *VMware* platformą. Atlikta virtualių mašinų integracija į *GNS3* platformą. Tai pat buvo sukonfigūruojama visi tinklo įrenginiai su tikslu atlikti *DHCP* protokolo atakas sklandžiai ir be jokių trikdžių. Stebėtas tinklo srautas atakų metu bei analizuojami ir renkami duomenys pasitelkiant duomenų ir tinklo stebėjimo įrankius.

3.3. Reikalavimai aparatūrai

Siekiant sukurti efektyvų *GNS3* tinklą ir naudoti *VMware* programą kuriant virtualizaciją ir atliekant *DHCP* protokolo atakas, aparatūros reikalavimai yra gana aukšti, kad butų užtikrintas reikiamas veikimo efektyvumas ir stabilumas. Pagrindiniai aparatūros reikalavimai:

1. Procesorius (*CPU*):
   - Rekomenduojama procesorius turintis daug branduolių, pavyzdžiui, Intel i7 ar AMD Ryzen 7, kuris galėtų efektyviai susidoroti su keletą virtualių mašinų ir *GNS3* sukurtų tinklų pajungtų vienu metu. Svarbu, kad procesorius palaikytų VT-x technologijas reikiamas virtualizacijai.
2. Operatyvi Atmintis (*RAM*)
   - Norint sklandaus veikimo rekomenduojama turėti mažiausiai 16 GB *RAM* tačiau jeigu planuojama vykdyti sudėtingesnius eksperimentus 16 GB gali pritrūkti. *RAM* dydis tiesiogiai veikia virtualių mašinų ir tinklų našumą, todėl kuo daugiau RAM tuo efektyviau galima atlikti bandymus.
3. Kietasis diskas (*SSD/HDD*)
   - Rekomenduojama kompiuteryje turėti *SSD* dėl greitesnių skaitymo ir rašymo operacijų, kurios pagerina ir pagreitina virtualių mašinų paleidimo laiką bei patį veikimą. Rekomenduojama mažiausiai 500 GB talpos jog būtų užtikrintas veikimas be trikdžių.

4. Tinklo plokštė
    - Rekomenduojama turėti *Gigabit Ethernet 1 Gbps* arba greitesne tinklo plokšte, kad būtų galima užtikrinti duomenų perdavimo greitį tarp *HOST* mašinos ir sukurtų virtualių mašinų, ypač atakų metu ir tinklo duomenų srauto stebėjimo metu.
5. Vaizdo plokštė (*GPU*)
    - *GNS3* ir *VMware* nepriklauso nuo didelio grafikos apdorojimo, tačiau rekomenduojama turėti bent jau *Geforce GTX 850m* ar panašaus stiprio plokštę jei naudojamas daugiau nei vienas monitorius.

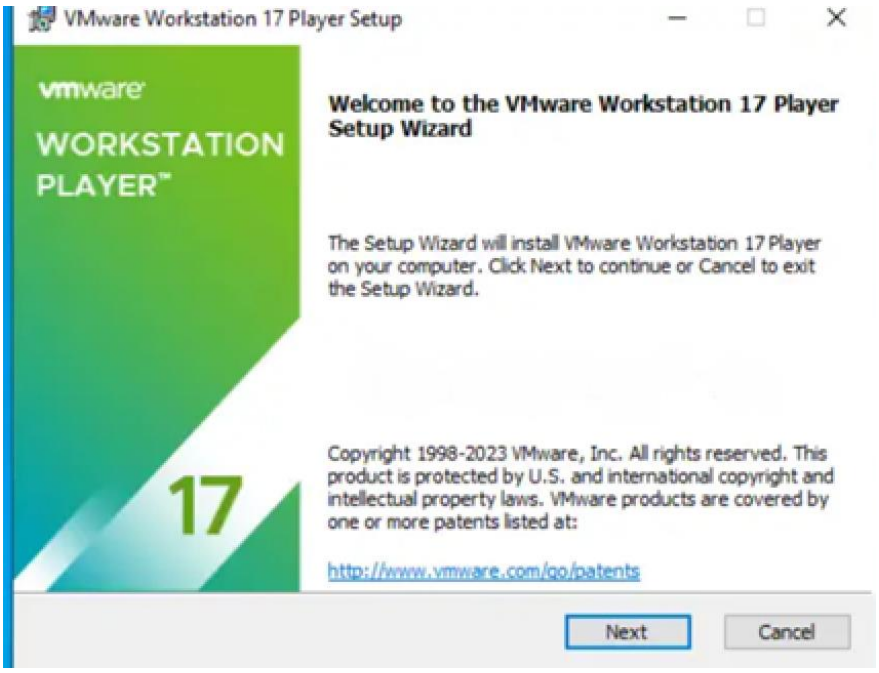
Siekiant efektyviai naudoti šią konfigūraciją kibernetinio saugumo testavimui, būtina įsitikinti, kad visi komponentai yra suderinti ir tinkamai sukonfigūruoti, kad išvengtumėte galimų aparatūros trikdžių ar našumo stokos.

3.4. *GNS3* ir *VMware* virtualios aplinkos įdiegimas ir parengimas

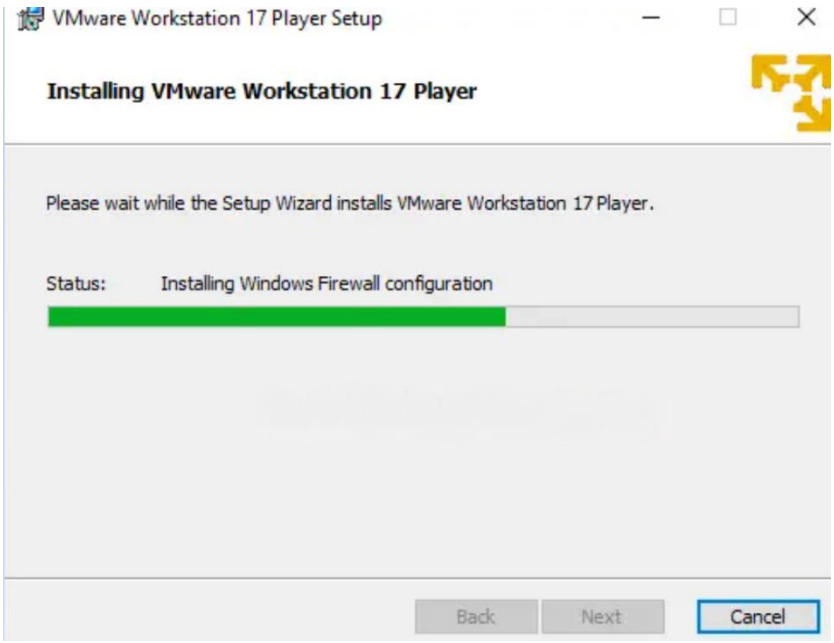
GNS3 ir *VMware* platformos sudiegtos ir paruošiamos nuosavame kompiuteryje, šios programos naudotos sukuriant virtualų tinklą ir atliekant *DHCP* protokolo atakas bei stebint tinklo duomenų srautą su tikslu išsiaiškinti silpnas įrenginių vietas ir netinkamas konfigūracijas, bei kaip apsisaugoti nuo atakų.

3.4.1. *VMware* Įdiegimas

VMware parsisiųsta iš *VMware*.com svetainės. Svetainėje pasirinkta nemokamas atsiuntimas ir versiją pagal savo kompiuterio parametrus ir operacinę sistemą. Atsisiusta *VMware* atidaromas įrašymo failas ir pradedama instaliaciją. Atsidarius instaliavimo langui spaudžiamas „Next“ mygtukas ir laukiama kol programa įrašomą. Įrašymo metu pasirenkama jog *VMware* bus naudojama ne komerciniam naudojimui.

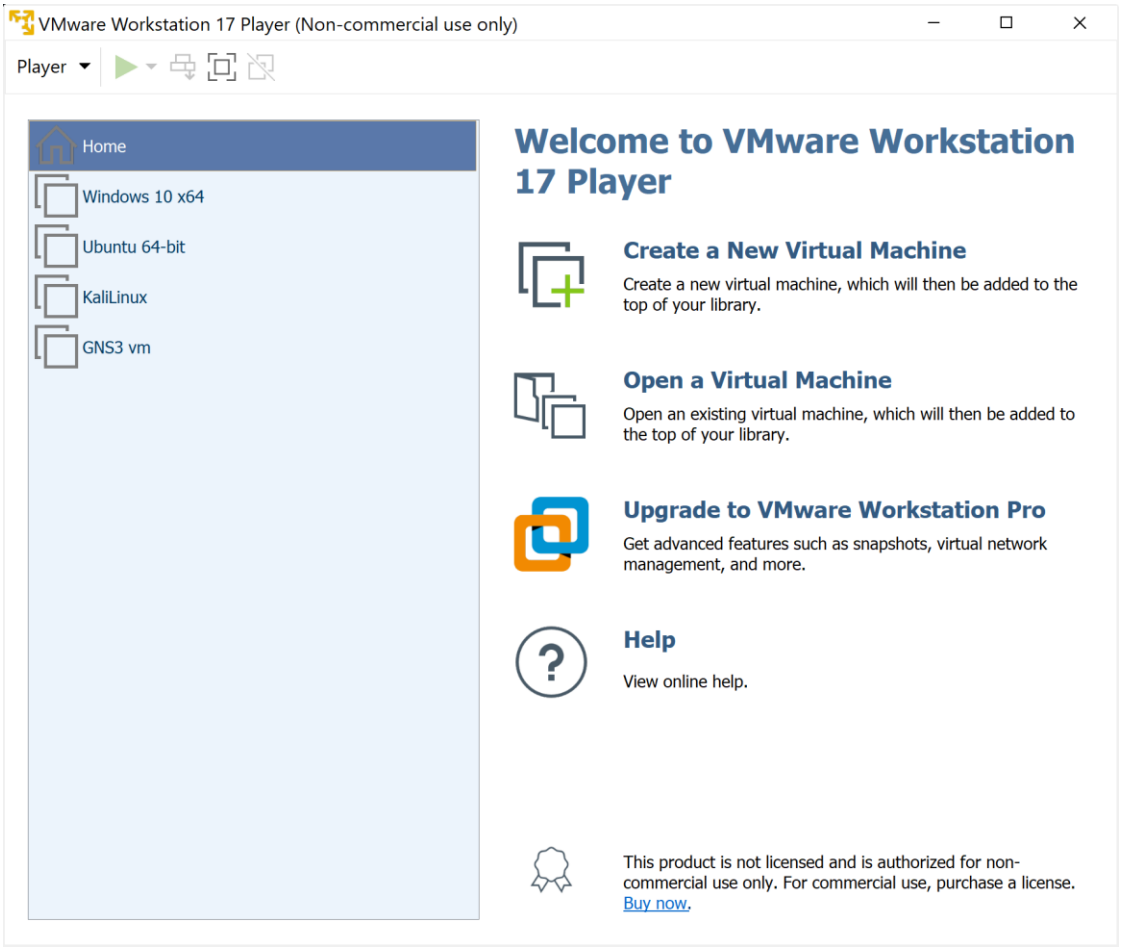


3.1 pav. VMware instaliacijos langas



3.2 pav. VMware instaliacijos eiga

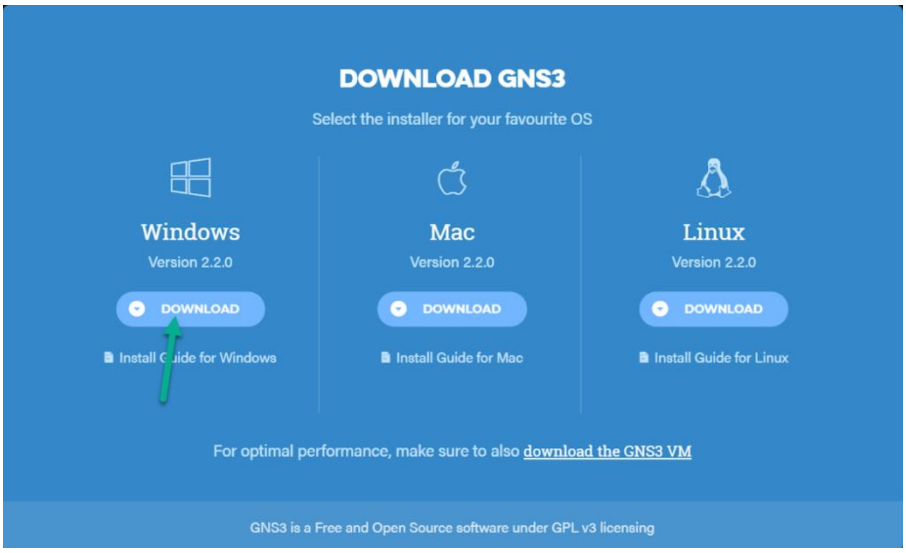
3.3 pav. VMware pasirinkimas, jog bus naudojama ne komerciniais tikslais



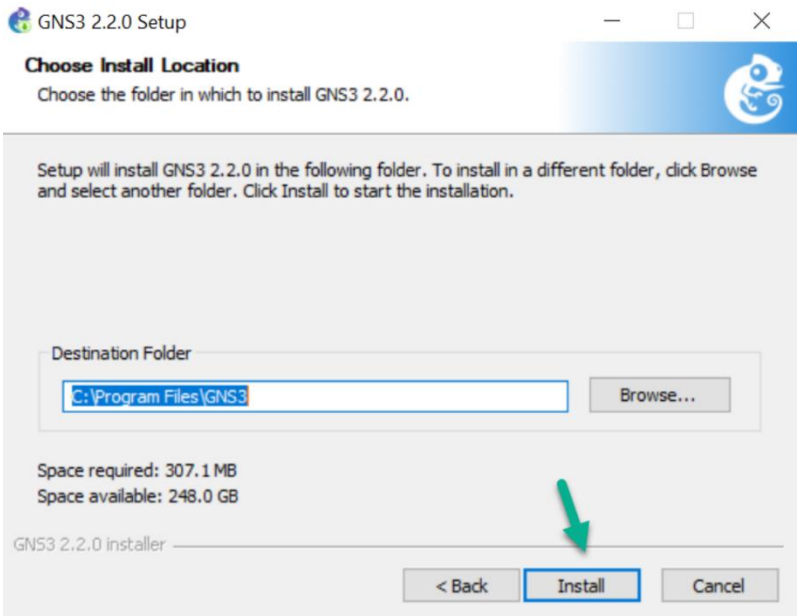
3.4 pav. Įrašytos programos vaizdas

3.4.2. *GNS3* Įdiegimas

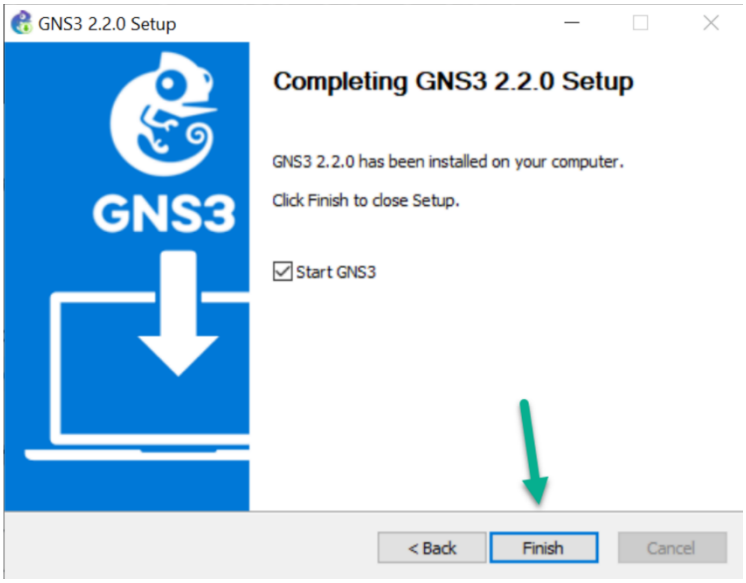
GNS3 platformą parsiųsta iš oficialios *GNS3* svetainės. Svetainėje pasirinkta *GNS3* versija pagal operacinę sistemą ir kompiuterio pajėgumus, parsiunčiama tvarkyklė ir atidaroma. Atsidarius *GNS3* tvarkyklei praeinami visi jos žingsniai pasirinkami reikiami punktai ir palaukiama kol viskas susirašys.



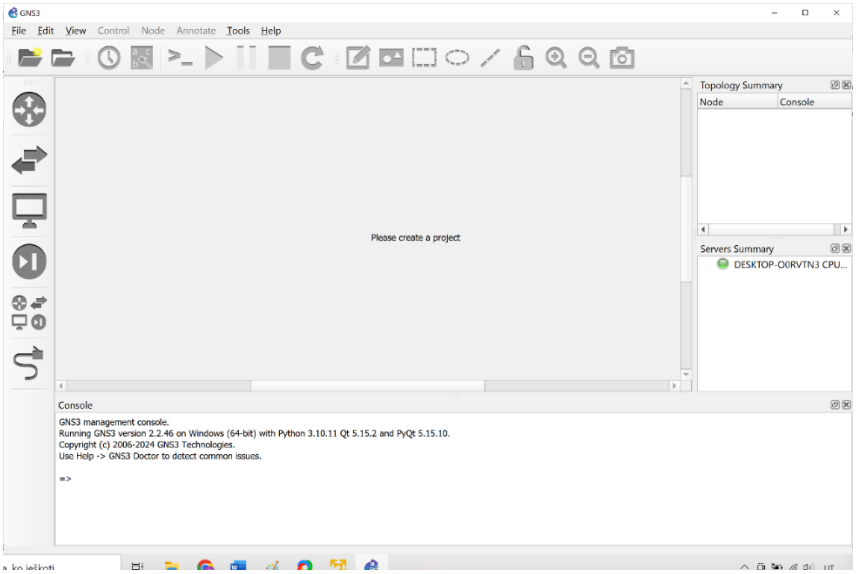
3.5 pav. GNS3 atsisiuntimas iš svetainės



3.6 pav. GNS3 įrašymo pradžia



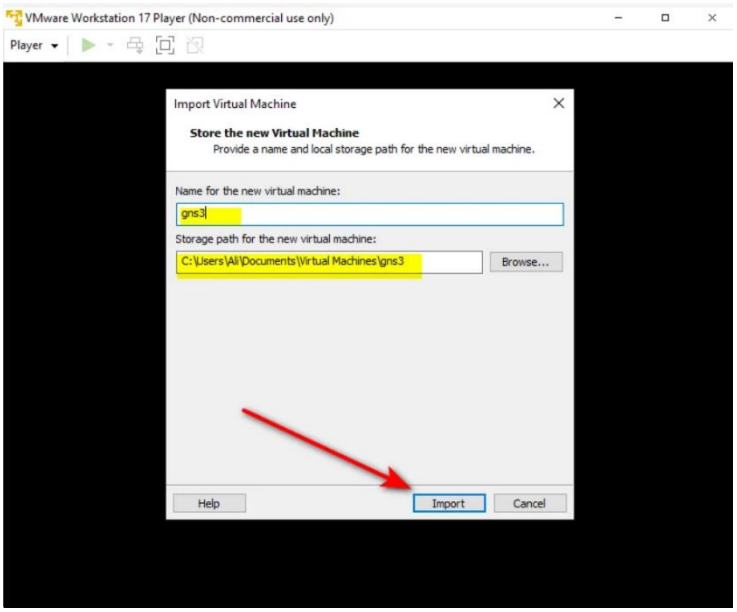
3.7 pav. GNS3 instaliacijos pabaiga



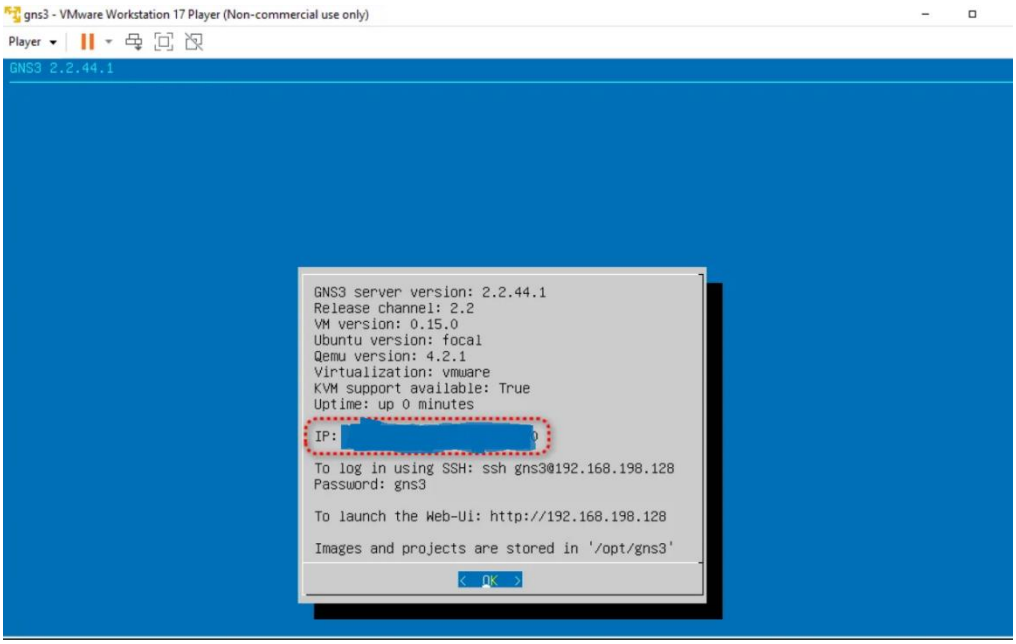
3.8 pav. GNS3 programos vaizdas

3.4.3. *GNS3* VM Įdiegimas

Įrašius *GNS3* ir *VMware* platformas svarbu taip pat įsirašyti ir *GNS3* VM, kad *GNS3* platforma palaikytų *VMware* ir būtų galima sukurtas virtualias mašinas įdiegti į *GNS3* platforma bei vėliau tiesiogiai prijungti ir naudoti virtualaus tinklo kūrime. Failas kuris parsiunčiamas bus .rar formatu, jis išarchyvuojamas, po to atidaromas *GNS3* VM failas, paleidus failą atsidarys *VMware* langas kuriame reikės nurodyti reikiama įrašymo informacija. Tada spaudžiamas „Import“ mygtukas. Kai *GNS3* VM idiegta galima naudotis *GNS3* ir *VMware* platformomis.



3.9 pav. GNS3 VM įrašymo eiga



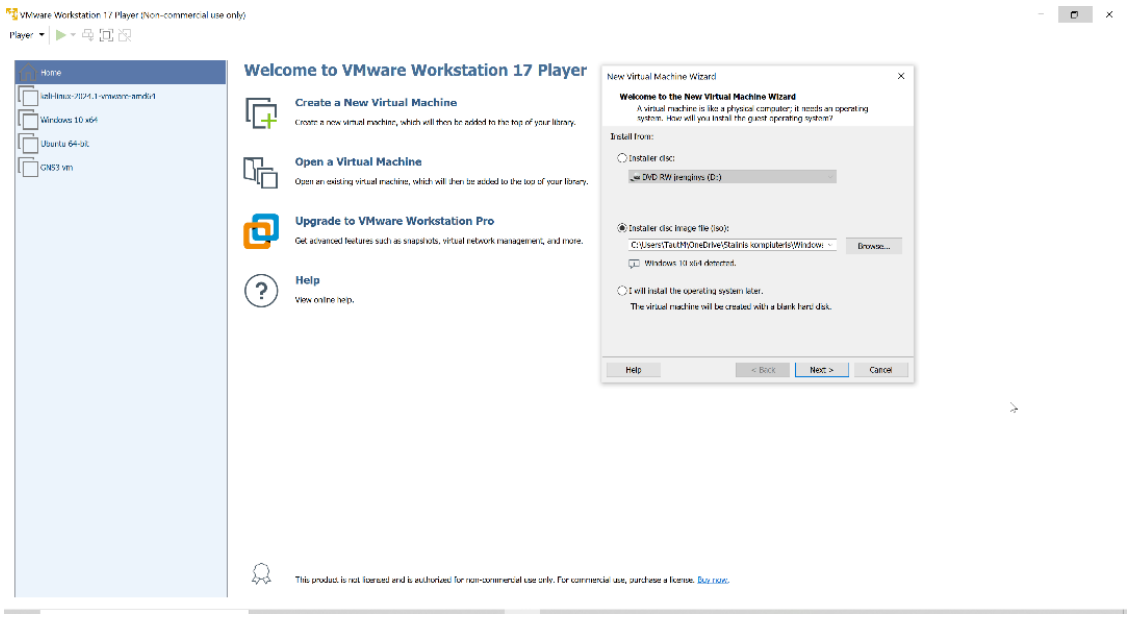
3.10 pav. GNS3 VM įrašyta

3.5. Serverių įdiegimas

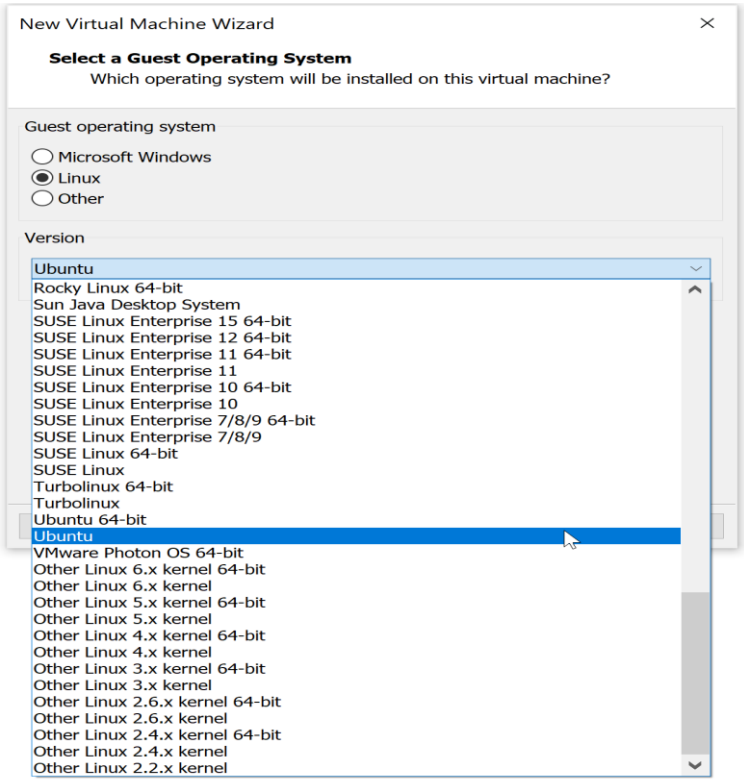
Šiam eksperimentui naudojami ir įrašomi keli serveriai vienas iš jų *Kali Linux*, kitas *Windows 10*. Abi operacinės sistemos yra būtinos norint atlikti šį eksperimentą, taip pat turi būti tinkamai sukonfigūruotos.

3.5.1. Naujos virtualios mašinos pridėjimas prie *VMware*

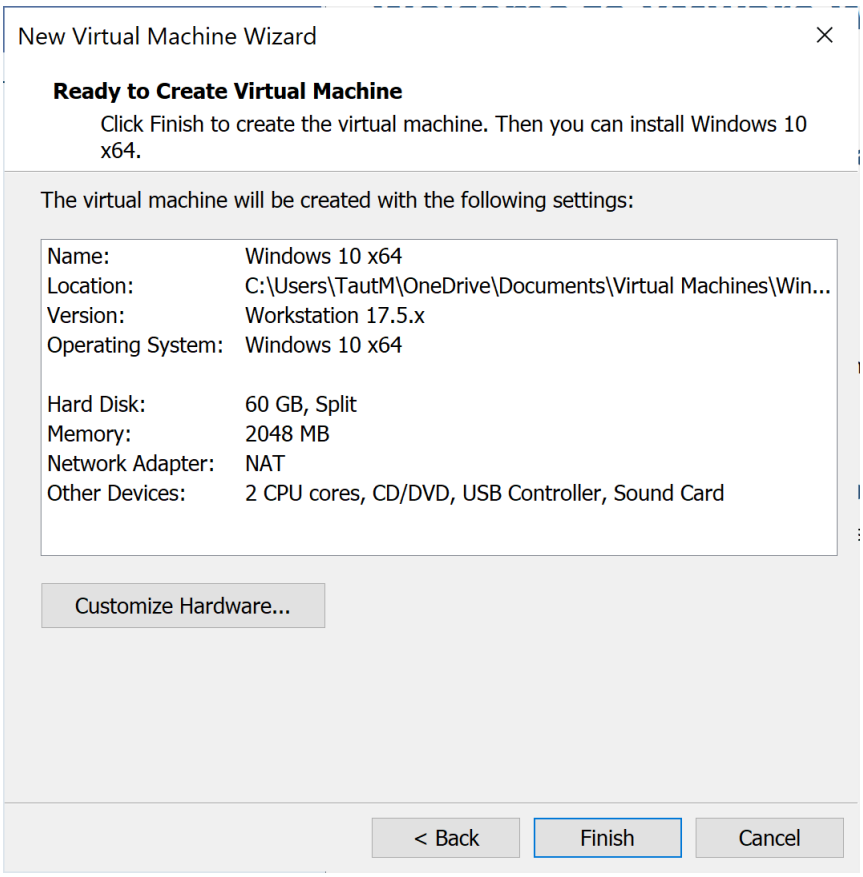
Norint įdiegti virtualią mašina reikalinga atsisiūsti reikiamą mašinos failą pritaikytą *VMware* platformai. Atsisiuntus failą atidaroma *VMware* ir spaudžiama „Create a New Virtual Machine“. Atsidarius naujam langui pasirenkamas failas su norima įdiegti mašina jei ji nebuvo automatiškai aptikta ir spaudžiama „Next“. Pasirenkama operacinė sistema ir versija, spaudžiama „Next“ , sukuriamas virtualios mašinos pavadinimas, pasirenkamos direktorijos kur bus įrašoma ir spaudžiama „Next“, Pasirenkama disko talpa ir spaudžiama „Next“, Peržiūrėjus visas konfigūracijas spaudžiama „Finish“.



3.11 pav. Virtualios mašinos pridėjimo eiga



3.12 pav. Operacinės sistemos pasirinkimas

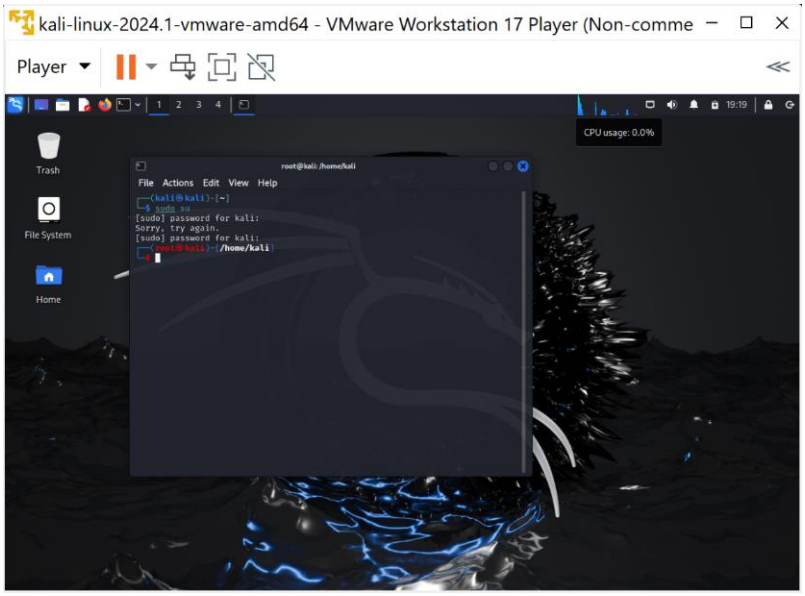


3.13 pav. Virtualios mašinos sukūrimo eiga

3.5.2. *Kali Linux* įdiegimas

Pirma įdiegta *Kali Linux* operacinė sistema *VMware* platformoje. Pradžiai reikėjo parsisiųsti *Kali Linux* ISO failą iš oficialios svetainės. Svetainėje pasirenkama „Installer Images“ tada pasirenkama reikiama versija ir parsiunčiama. Tada pridedama virtuali mašina prie *VMware* – žiūrėti skyrių „3.5.1 Naujos virtualios mašinos pridėjimas prie *VMware*“. Tai padarius įsijungiama pridėta virtuali mašina. Atsidariusiame „BIOS mode“ pasirenkama „Install“. Šis pasirinkimas instaliuos *Kali Linux* be grafinės sąsajos. Praeinama visi *Kali Linux* instaliavimo procesai ir susiinstaliuojama *Kali Linux*. Tai padarius operacinė sistema persikraus ir priklausomai nuo pasirinkimų instaliavimo procesuose įsijungs *Kali Linux* darbalaukis. *Kali Linux* operacinė sistema paruošta naudojimui.

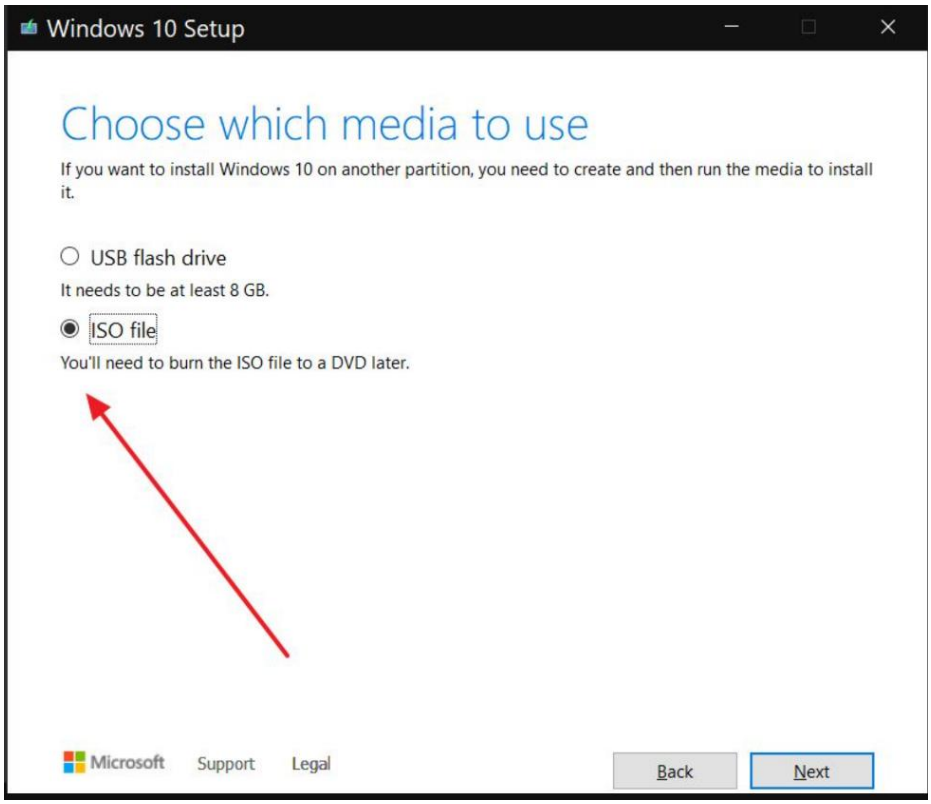
3.14 pav. Kali Linux BIOS aplinka



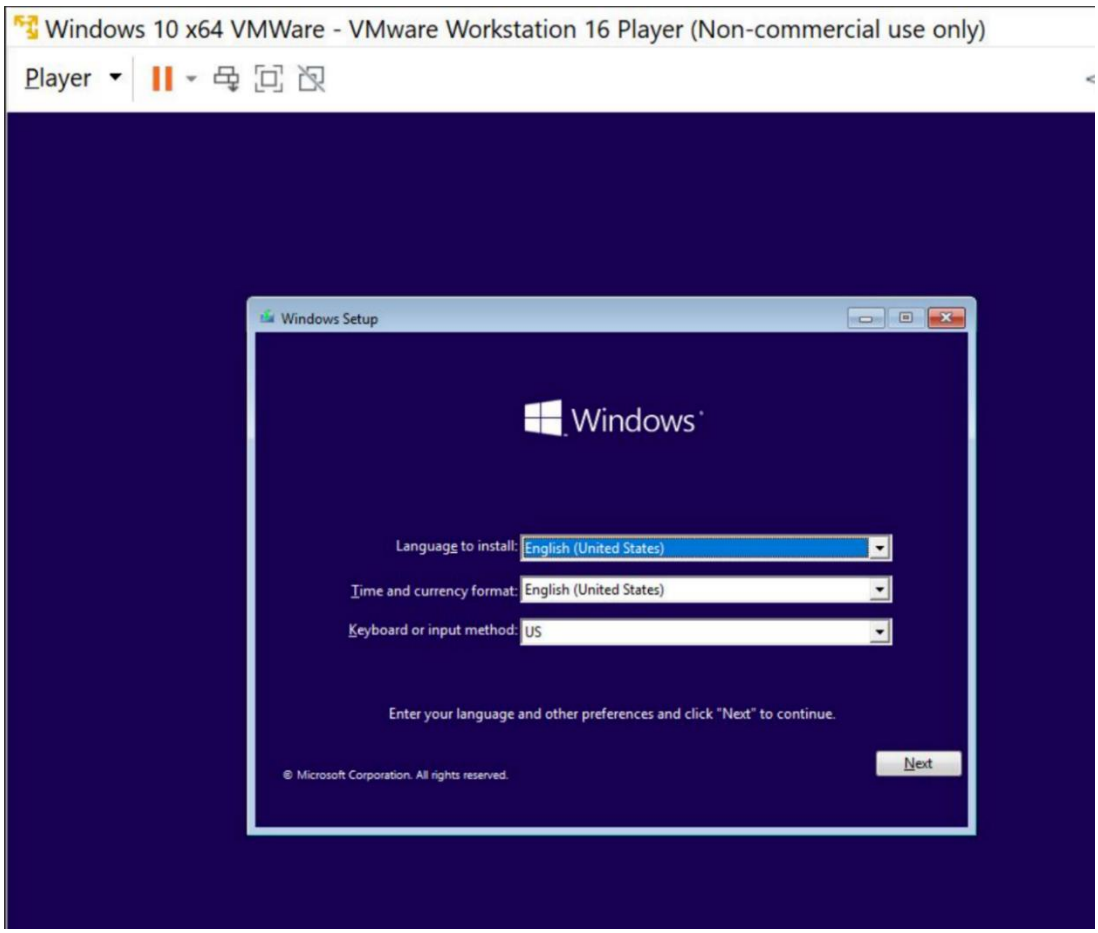
3.15 pav. Kali Linux aplinkos vaizdas

3.5.3. *Windows 10* įdiegimas

Galiausiai įdiegiama MS *Windows 10* operacinė sistema *VMware* platformoje. Pradžiai parsisiunčiama MS *Windows 10* ISO failas iš oficialios svetainės. Svetainėje pasirenkama reikiama versija ir parsisiunčiama. Tada pridedama virtuali mašina prie *VMware* – žiūrėti skyrių „3.5.1 Naujos virtualios mašinos pridėjimas prie *VMware*“. Tai padarius įsijungiama pridėta virtuali mašina. Įsijungus virtualiai mašinai automatiškai pradėjo diegtis *Windows 10*. Po greito operacinės sistemos susidiegimo įsijungs sąranka, kurioje reiks pasirinkti įvairius *Windows* nustatymus, tokius kaip kalbą, regioną ir t.t. Praeinami visi *Windows* sąrankos procesai ir baigiami instaliuoti *Windows*. Tai padarius operacinė sistema persikraus ir įsijungs *Windows* darbalaukis. *Windows* operacinė sistema paruošta naudojimui.



3.16 pav. Windows ISO failo atsisiuntimas



3.17 pav. Windows sistemos diegimas VMware platformoje

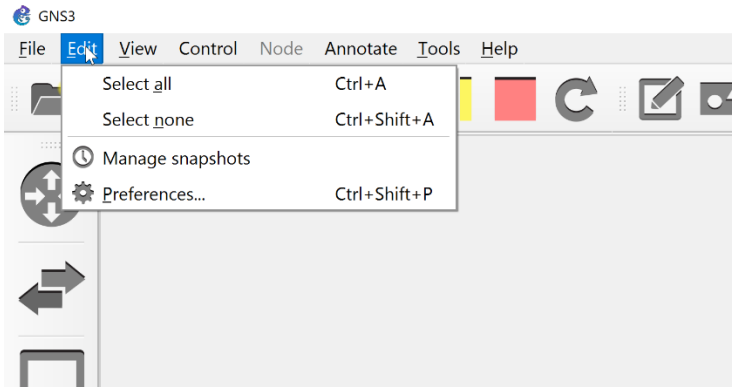
3.5.4. Apibendrinimas

Sudiegta du serveriai su skirtingomis operacinėmis sistemomis viena iš jų *Kali Linux*, kita *Windows 10*. Serveriai buvo sudiegti *VMware* platformoje ir joje virtualizuojami. Serveriai sudiegti su grafinėmis sąsajomis.

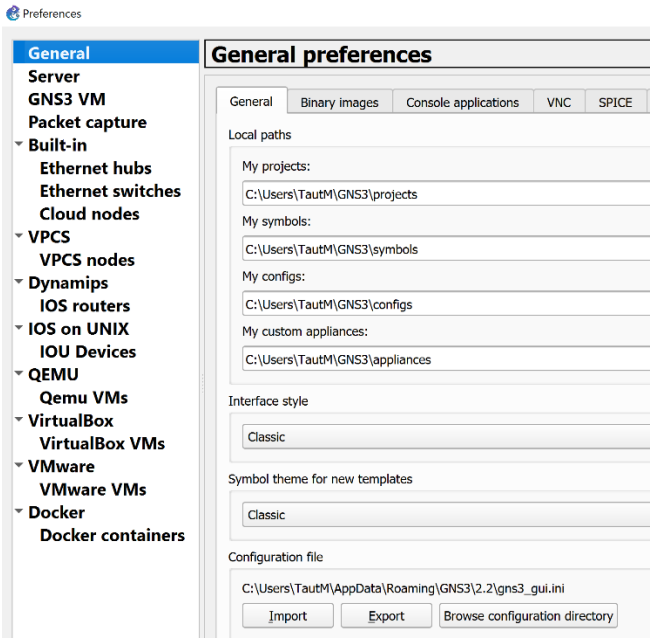
3.6. Topologijos sukūrimas *GNS3* aplinkoje

3.6.1. *VMware* virtualių mašinų pridėjimas į *GNS3* platformą

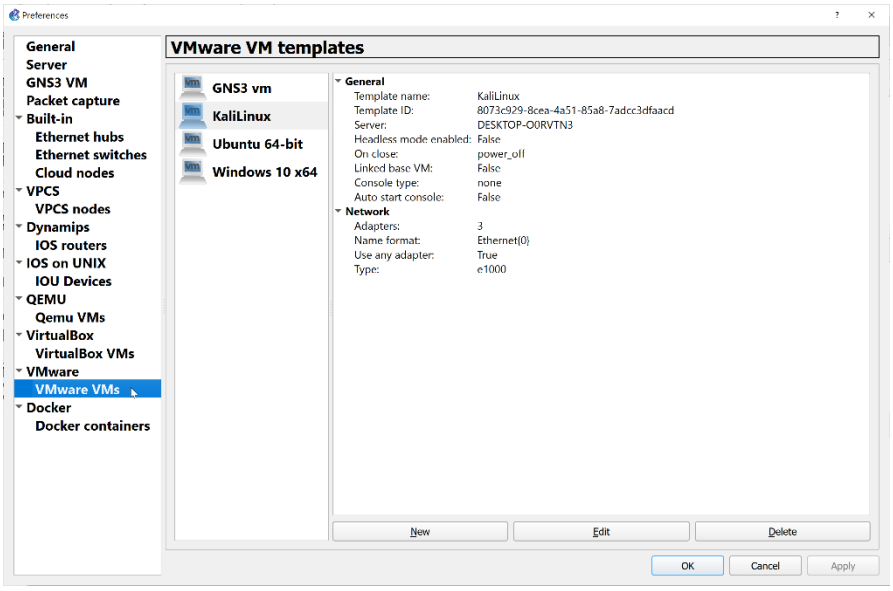
Pradedant naudotis *GNS3* atviro kodo programa svarbu integruoti jau sudiegtas virtualias mašinas. Kadangi *GNS3* yra galimybė integruoti VM iš *VMware* užtenka pereiti kelis paprastus pridėjimo žingsnius, jog būtų integruotos virtualios mašinos. Pasijungiamas *GNS3* spaudžiama „Edit“, tada pasirenkama „Preferences“, spaudžiama „*VMware*s VMs“ tada „New“, pasirenkama norima virtuali mašina ir spaudžiama „Finish“



3.18 pav. GNS3 "Edit" mygtukas



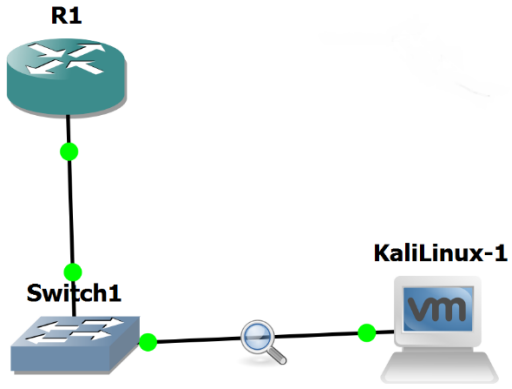
3.19 pav. GNS3 "Preferences" aplinka



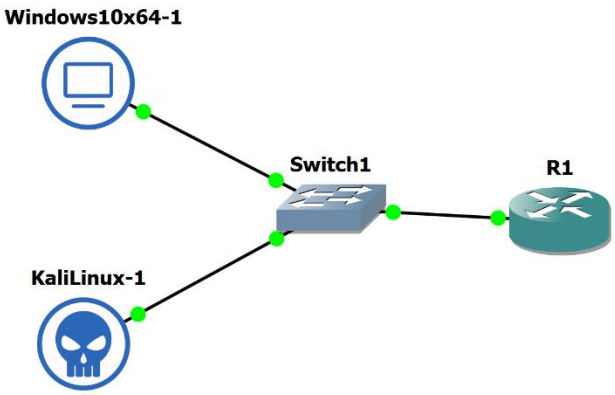
3.20 pav. GNS3 Virtualių mašinų koregavimo aplinka

3.6.2. Topologijos sukūrimas

Kuriama tinklo topologija, prieš kuriant topologiją reikia atsižvelgti į tai ką norimą daryti, kam ji bus naudojama ir kokių komponentų tam reikės. Topologiją sudarė vienas maršrutizatorius, vienas komutatorius ir vienas atakuojantis kompiuteris, šie komponentai buvo naudojami vienai atakai atlikti. Kitai atakai atlikti reikia pridėti dar vieną papildomą kompiuterį. Prieš pradedant darbą reikia atitinkamai sukonfigūruoti įrenginius pagal atliekamą ataką, bei įrašyti trūkstamus komponentus į virtualias mašinas.



3.21 pav. DHCP Starvation atakos topologija



3.22 pav. DHCP Rogue Server atakos topologija

3.6.3. Apibendrinimas

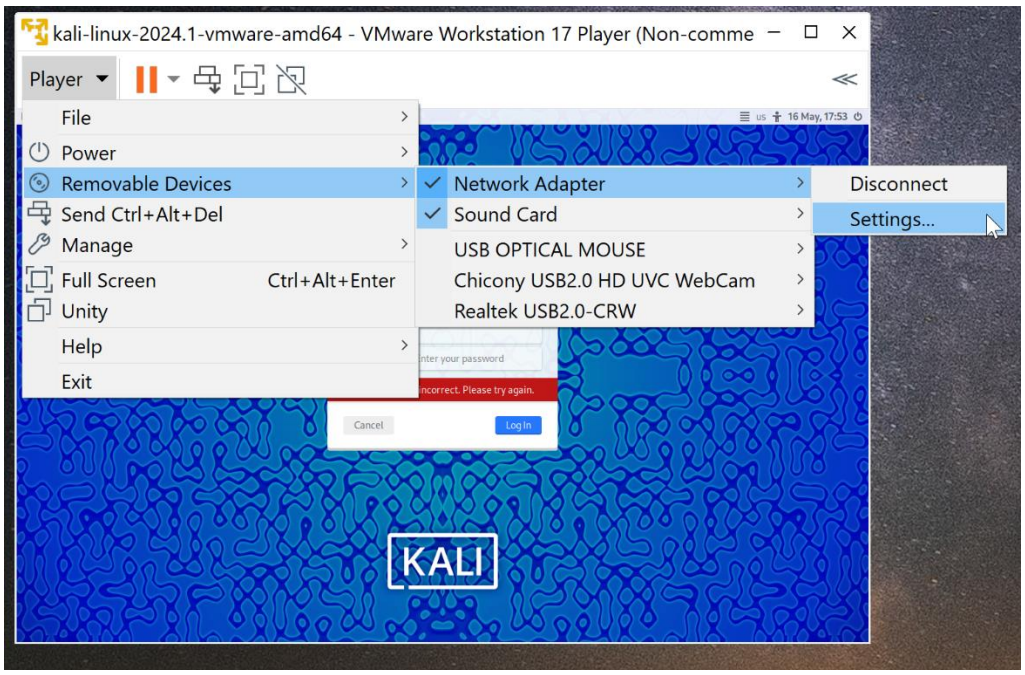
GNS3 aplinkoje buvo pridėtos VMware virtualios mašinos, kad būtų galima tiesiogiai jas naudoti kuriant virtualų tinklą. Ši kombinacija suteikia galimybę tiksliai modeliuoti realias tinklo sąlygas ir atlikti įvairias saugumo testavimo procedūras. Sukurta tinklo topologija apėmė kelis esminius komponentus: atakuojantis kompiuteris su Kali Linux operacine sistema, vartotojo kompiuteris su Windows 10 operacine sistema, taip pat maršrutizatoriai ir komutatoriai. Kali Linux operacinė sistema, esanti atakuojančiame kompiuteryje, yra žinoma dėl savo saugumo testavimo įrankių gausos, leidžiančios vykdyti įvairias kibernetines atakas ir pažeidžiamumų analizę. Vartotojo kompiuteris su Windows 10 operacine sistema buvo naudojamas kaip pagrindinis atakų taikinys, siekiant imituoti realias vartotojo aplinkos sąlygas.

Maršrutizatoriai ir komutatoriai buvo integruoti į tinklo topologiją, siekiant užtikrinti tinklo ryšį ir maršrutizavimo funkcijas. Šie įrenginiai padėjo modeliuoti sudėtingesnes tinklo struktūras ir atlikti išsamesnius saugumo testus. Naudojama konfigūracija apėmė tinklo įrenginių paruošimą atakoms, įskaitant IP adresų priskyrimą, tinklo taisyklių nustatymą ir kitų reikiamų parametrų konfigūravimą. Ši virtuali aplinka suteikė galimybę saugiai atlikti kibernetinių atakų simuliacijas ir analizuoti jų poveikį, nepažeidžiant realių svetainių ar vartotojų kompiuterių, užtikrinant privatumo politikos laikymąsi ir tinklo saugumą.

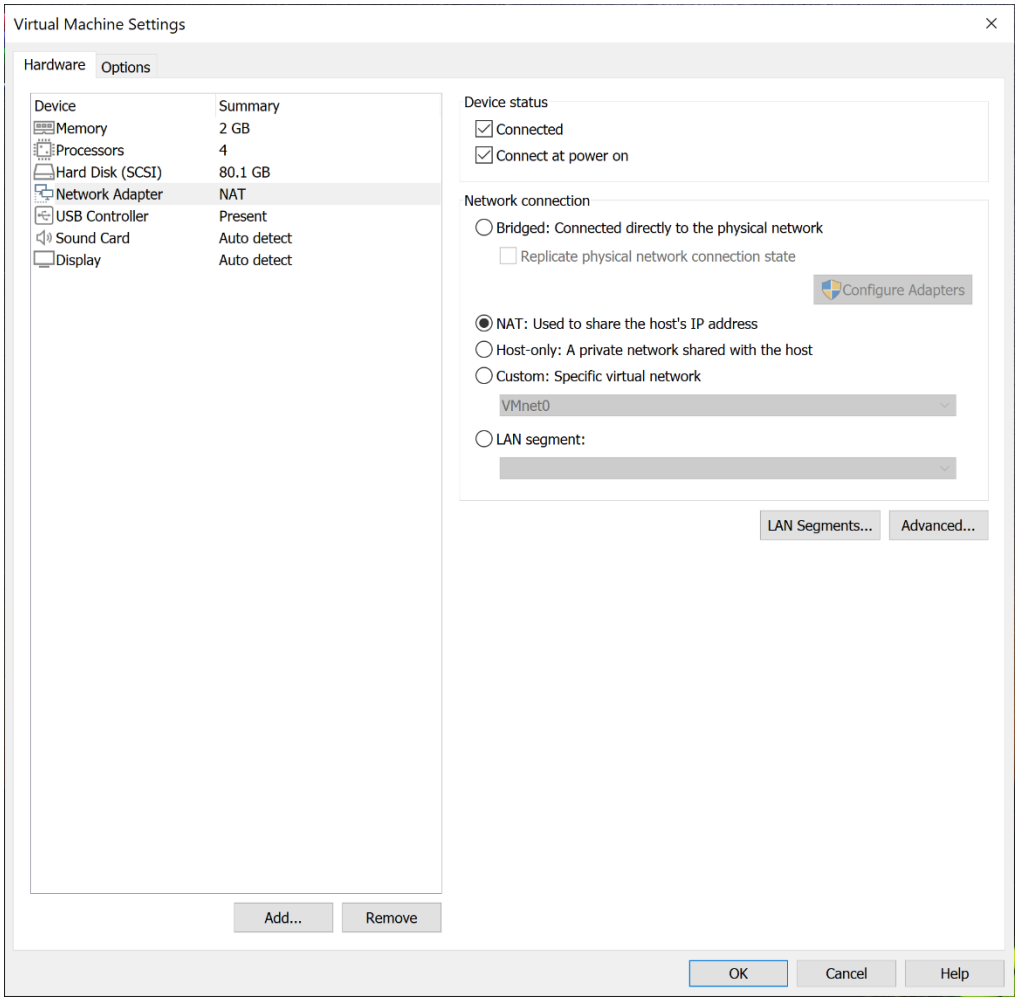
3.7. Sistemos konfigūravimas

3.7.1. Virtualių mašinų interneto adapterių konfigūracija

Atakoms atlikti reikalingas interneto ryšys, tam kad jį turėti reikia sukonfigūruoti virtualių mašinų adapterius. Tai galima padaryti per GNS3 paleidus virtualias mašinas. Pasijungus virtualiai mašinai atidaromas VMware langą ir spaudžiama „Player“ mygtukas, tada „Removable devices“, toliau - „Network Adapter“ ir galiausiai „Settings“. Atlikus šiuos veiksmus atidaromas virtualios mašinos nustatymų langas ir pasirenkamas „Hardware“, matomas „Network Adapter“ ir prie „Network Connection“ skilties pasirenkamas „NAT“ adapteris. Interneto pajungimas gali užtrukti šiek tiek laiko, atlikus visus veiksmus einama į virtualią mašiną ir bandoma pajungti, pvz: google.



3.23 pav. Kelias iki adapterio nustatymų



3.24 pav. Interneto adapterių nustatymo langas

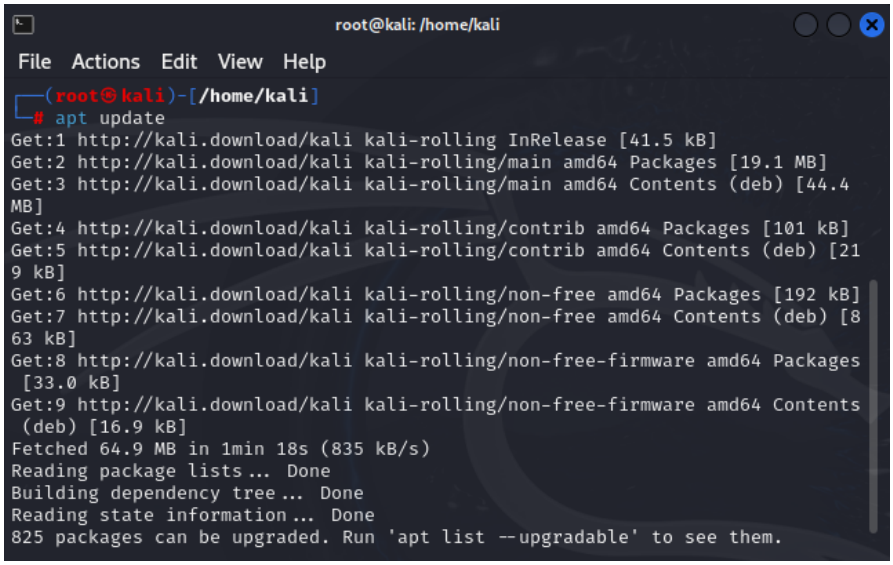
3.7.2. Apibendrinimas

Tinklo adapterių konfigūracija būtina norint, kad virtualios mašinos galėtų prisijungti į tinklą bei komunikuoti tarpusavyje.

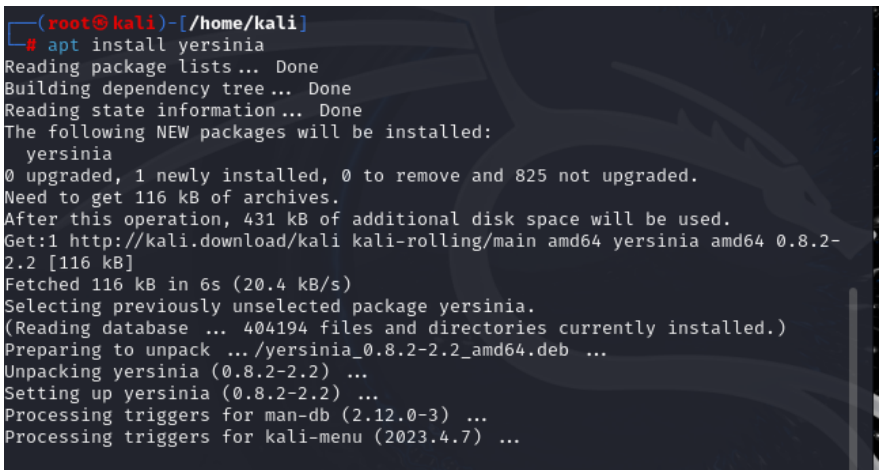
3.8. Įrankių įdiegimas

3.8.1. *Yersinia* diegimas į *Kali Linux*

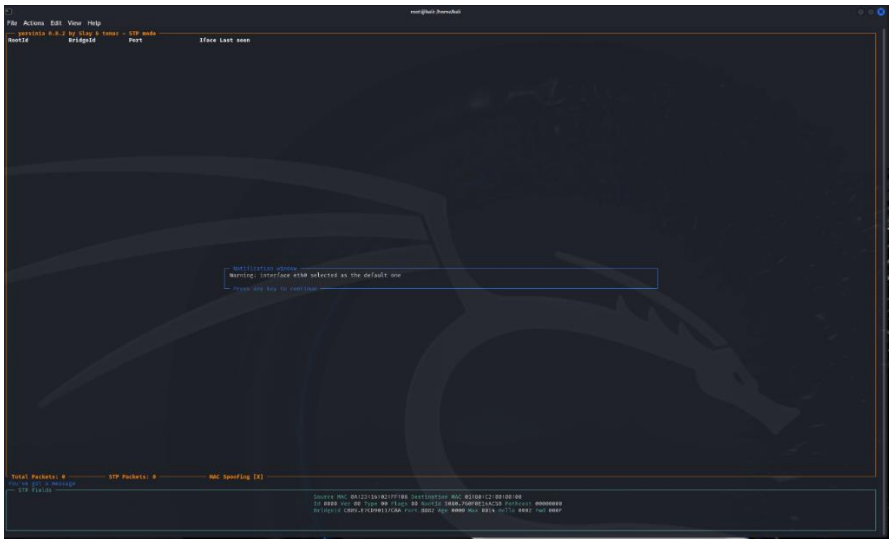
Vienai iš atakų atlikti reikalingas „*Yersinia*“ programos paketas. Šį paketą į operacinę sistemą reikėjo įsidiegti pačiam. Visų pirma, atidaromas terminalas, rašoma „sudo su“. Tada įvedamas slaptažodis, vėliau atnaujinami paketai su komanda „apt update“. Toliau rašoma „apt install *Yersinia*“. Pasibaigus diegimui rašoma „*Yersinia* -I“ ir atidaroma programos aplinka.



3.25 pav. Kali Linux "apt update" komanda



3.26 pav. Yersinia diegimo procesas



3.27 pav. Yersinia aplinka

3.8.2. Apibendrinimas

Kali Linux sistemoje įdiegta *Yersinia* atakavimo programa su kuria atliekamos atakos tokios kaip *DHCP Starvation* ataka.

3.9. Išvados ir apibendrinimai

1. Sukurta sistemos archtektūra kurioje naudojama *VMware* ir *GNS3* programos.
2. Sukurta tinklo topologija su *GNS3* atviro kodo programa. Integruotos virtualios mašinos į *GNS3* programą.
3. Pateikti pagrindiniai reikalavimai aparatūrai norint dirbti sklandžiai ir be jokių trikdžių.
4. Nuosavame kompiuteryje įdiegtos *GNS3* ir *VMware* programos.
5. *VMware* programoje įdiegta *Kali Linux* virtuali mašina ir *Windows 10* virtuali mašina.

6. Virtualios mašinos integruotos į *GNS3* programą bei sukurtas virtualus tinklas su integruotomis mašinomis, kuriame buvo atliekamos *DHCP* protokolo atakos.
7. Sukonfigūruoti tinklo adapteriai, kad virtualios mašinos galėtų prisijungti į tinklą ir komunikuoti viena su kita.

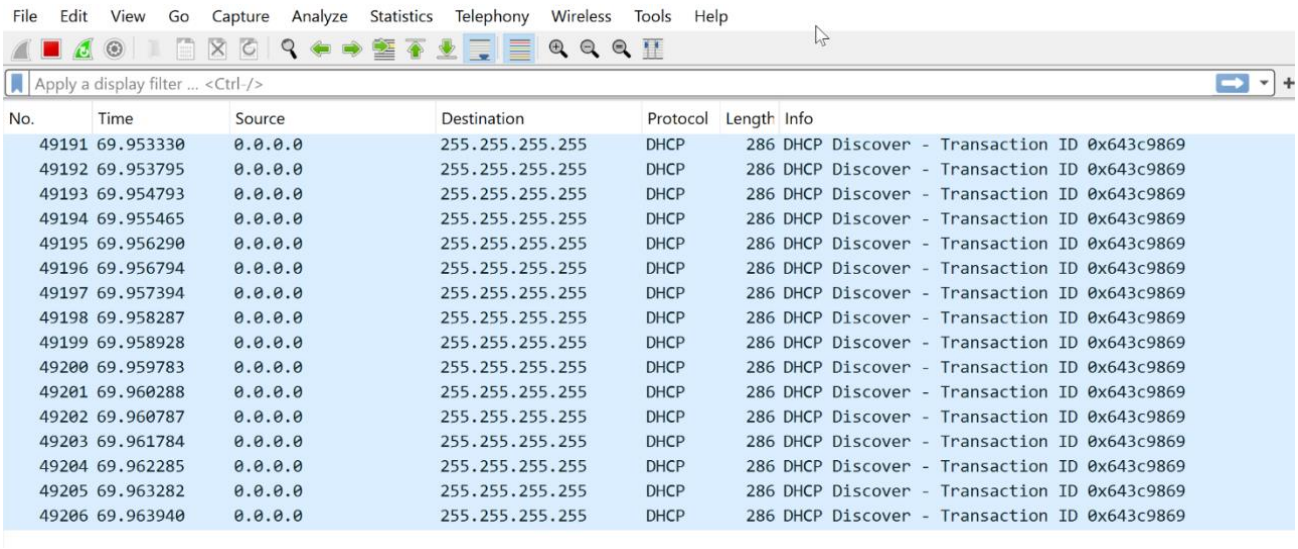
4. EKSPERIMENTINĖ IR PRAKTINĖ DALIS

4.1. Simuliacinės aplinkos parengimas

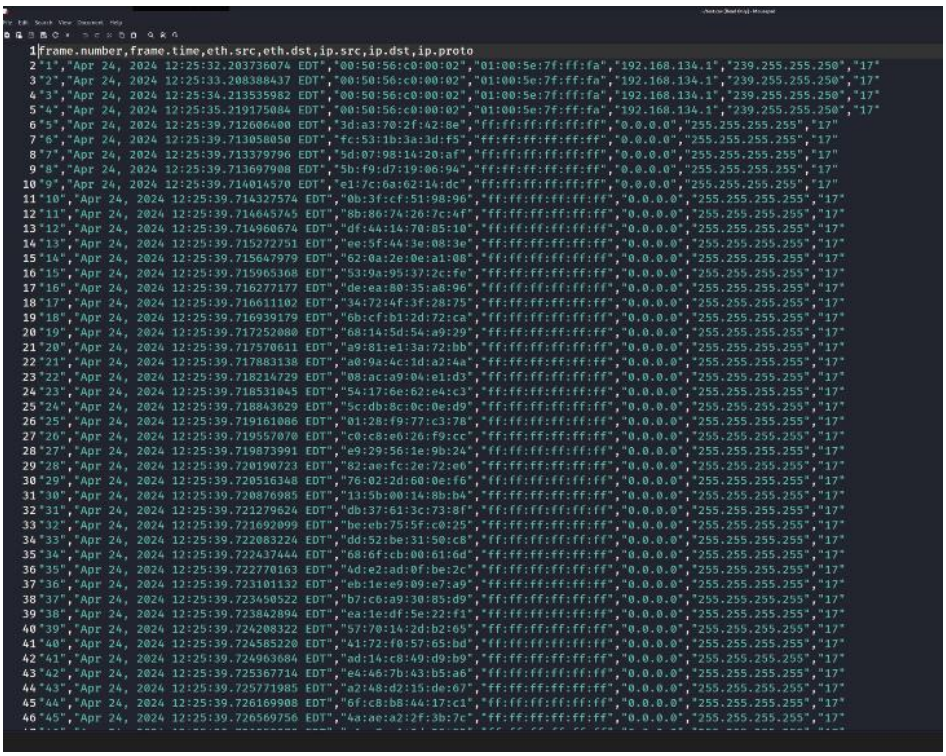
Prieš pradedant eksperimentą ir atliekant atakas įsitikinta, jog visos virtualios mašinos yra įjungtos ir turi ryšį tarpusavyje. *GNS3* (*GNS3* n.d.) platformoje pajungtas tinklas ir pajungtos virtualios mašinos. Sukonfigūruoti interneto adapteriai ir patikrintas ryšys *Kali Linux* (*Kali Linux* n.d) platformoje, pajungtas terminalas ir komandinėje eilutėje rašoma „ping“ bei *Windows 10* kompiuterio IP adresas. Ta pačia eiga ir per *Windows* kompiuterį su cmd komandine eilute.

4.2. Duomenų rinkimas

Duomenų rinkimui buvo naudota pagrindinis tinklo stebėjimo įrankis, t.y. „*WireShark*“, surinkus tinklo srauto duomenis ir siunčiamus paketus galima analizuoti duomenis ir panaudoti juos mašininiam mokymui.



4.1 pav. WireShark aplinka ir DHCP Discover paketai



4.2 pav. TShark duomenų rūšiavimas

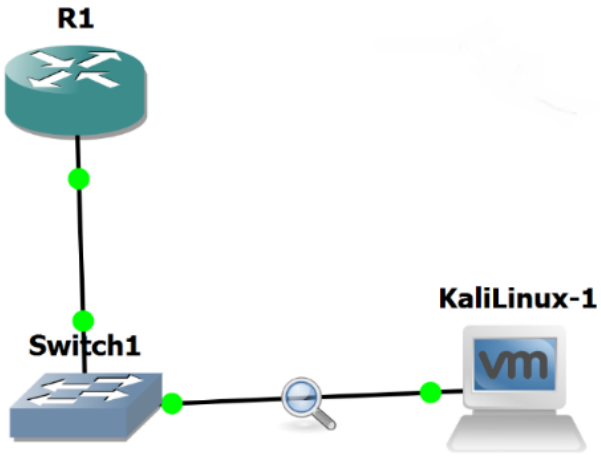
Taip pat buvo naudojamas „*TShark*“ (*TShark* n.d) įrankis, kuris leidžią pasirinkti, kokius tinklo duomenis ir paketus rinkti, šis įrankis pagelbėja tuo, jog skirtingai nei *WireShark* galima pasirinkti tik tam tikrus duomenis ir nereikia ieškoti reikiamų duomenų tarp daugumos nereikalingų. Duomenys kurie buvo surinkti, pateikiami CSV formato failais, kurie lengvai tvarkomi analizės įrankiuose ir naudojami mašininiam mokymuisi.

4.3. Simuliacija

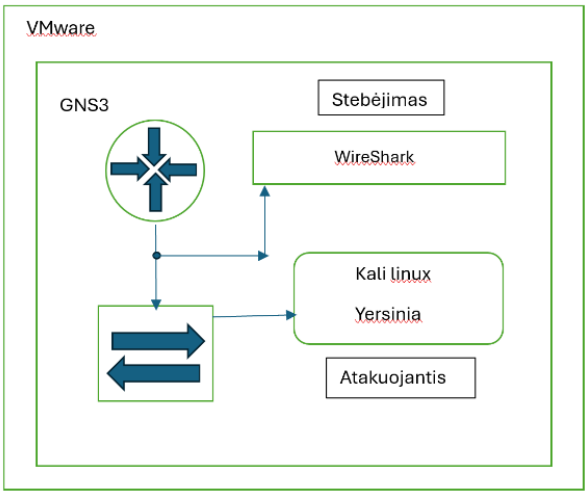
Platformoje sukurta tinklo topologija *GNS3* leidžianti atlikti *DHCP Starvation* ataką, aprašomos informacijos detalės ir simuliacijos eiga.

4.3.1. *DHCP Starvation* ataka

Atakai naudojama topologija (1 pav.) kuri **s**udaryta iš vieno *cisco* maršrutizatoriaus, kuris naudojamas kaip *DHCP* serveris, vieno komutatoriaus ir atakuojančio kompiuterio su *Kali Linux* (*Kali Linux*, n.d.) platforma ir *Yersinia* programa. Šių įrankių pagalba, atliekama *DHCP Starvation* ataka su tikslu surinkti duomenis mašininiam mokymui.



4.3 pav. GNS3 topologija



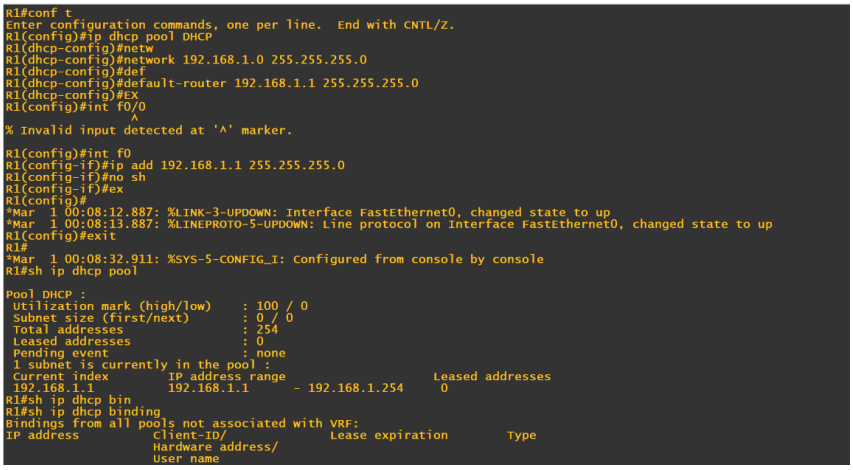
4.4 pav. Topologijos architektūra

Viena iš atakų - *DHCP Starvation* ataka. Tai agresyvi kliento ar įrenginio ataka, kurios metu įrenginys prisiima daugybę *DHCP* adresų iš serverio. Atakuojantis siunčia daugybę *DHCP* užklausų, siekdamas išnaudoti visus ar didžiąją dalį *DHCP* adresų, paliekant kitus klientus be tinklo ryšio. Ši ataka persidengia su „*spoofing*“ atakomis, kai kiti klientai negali gauti galiojančių IP adresų. Dėl šios priežasties klientų įrenginiai negali gauti IP adreso ir prieigos prie tinklo.

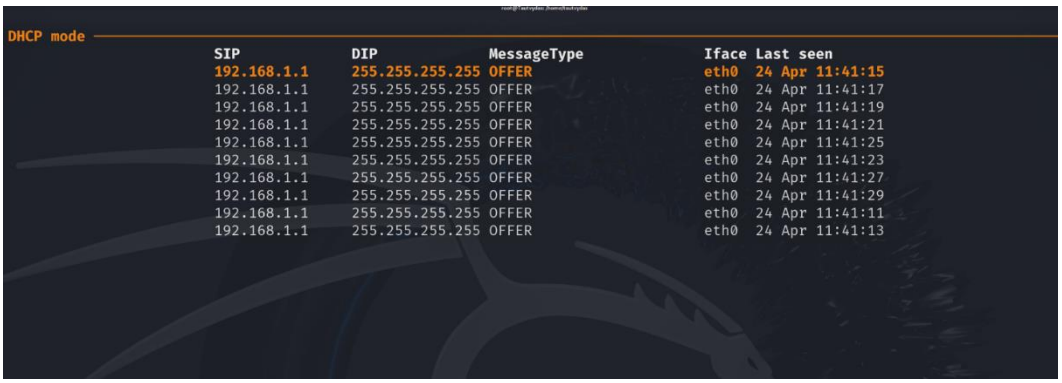
4.3.2. *DHCP Starvation* atakos simuliacijos eiga

Atsisiųstos *GNS3* ir *VMware* platformos, tada *GNS3* pagalba sukurta tinklo topologija (30 pav.), leidžianti atlikti atakas. Pradžioje konfigūruotas R1 maršrutizatorius, priskirtas IP adresas ir sukurtas IP adreso pool, tačiau pool'e nėra jokių IP adresų. Nustatomos IP adresų ribos nuo

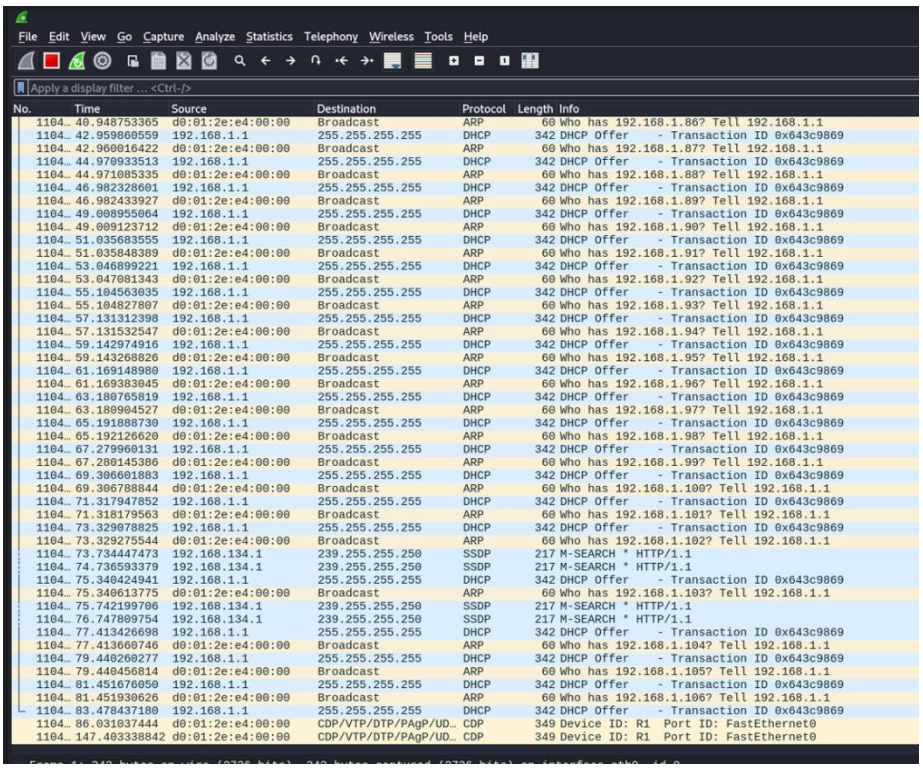
192.168.1.1 iki 192.168.1.254 (32 pav.). Po konfigūravimo atakuojančio *Kali Linux* terminale įvedama "sudo su" ir slaptažodis. Terminale rašoma "*Yersinia* -I" komanda ir atidaroma programos aplinka (33 pav.). Spaudžiama "g" raidė ir pakeičiama aplinka, matoma R1 siunčiamos offer užklausos (33 pav.). Paspausta "x" ir pasirinkta ataka skaičiumi 1, pradėti siųsti klaidingi IP adresai. *GNS3* atidarytas, jungtis tarp R1 ir komutatoriaus ("Switch") pažymėta, pasirinkta "Capture" ir stebėti siunčiami paketai naudojant *WireShark (35 pav.)*. Atidarytas naujas terminalas *Kali Linux*, naudojant "*TShark*" generuojami duomenys. Po kelių sekundžių ataka sustabdyta, spaudžiant "K", vėliau - "Y". Matoma, kad R1 turėjo 105 naujus IP adresus, palyginta su pradiniu 0 (36 pav.). Duomenų generavimui naudotas *TShark*, suvedama komanda į *Kali Linux* terminalą: *TShark* -T fields -e frame.number -e frame.time -e eth.src -e eth.dst -e ip.src -e ip.dst -e ip.proto -E header=y -E separator=, -E quote=d -E occurrence=f > test.csv. (37 pav.) Pateikiamos nuotraukos bendram supratimui.



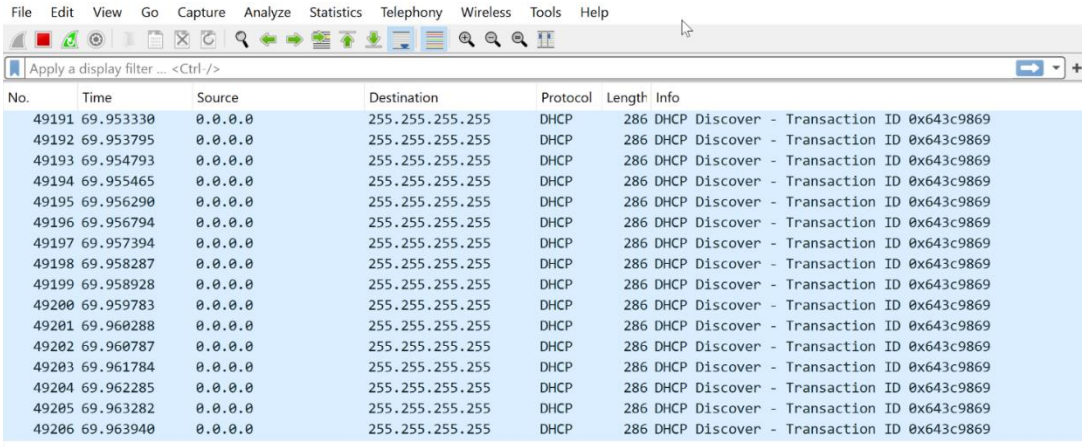
4.5 pav. Maršrutizatoriaus konfigūracija



4.6 pav. Offer paketai Yersinia aplinkoje



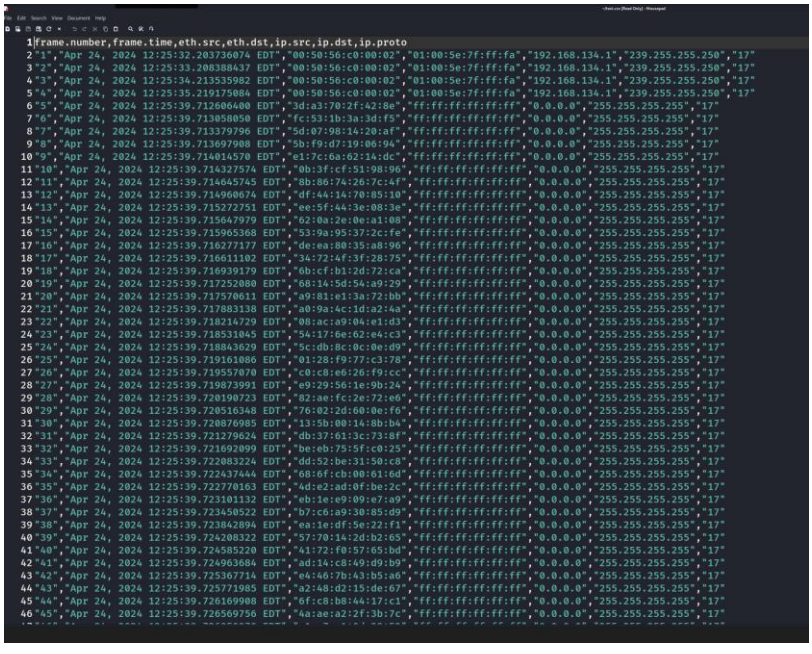
4.7 pav. WireShark programoje siunčiami paketai atakos metu



4.8 pav. Klaidingi paketai siunčiami atakos metu

```
 192.168.1.107        192.168.1.1       - 192.168.1.254     105
R1#sh ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/                  Lease expiration        Type
                    Hardware address/
                    User name
192.168.1.2         2155.e47a.4c24              Mar 01 2002 12:14 AM    Automatic
192.168.1.3         645d.535c.b41b              Mar 01 2002 12:14 AM    Automatic
192.168.1.4         3168.8846.9c91              Mar 01 2002 12:14 AM    Automatic
192.168.1.5         b0f4.9907.15b4              Mar 01 2002 12:14 AM    Automatic
192.168.1.6         5fee.2d0b.27c8              Mar 01 2002 12:14 AM    Automatic
192.168.1.7         f4ce.9b63.dfc9              Mar 01 2002 12:14 AM    Automatic
192.168.1.8         9c26.8273.968d              Mar 01 2002 12:14 AM    Automatic
192.168.1.9         c751.265c.2321              Mar 01 2002 12:14 AM    Automatic
192.168.1.10        7e97.984d.3beb              Mar 01 2002 12:15 AM    Automatic
192.168.1.11        c21a.9b7b.ed10              Mar 01 2002 12:15 AM    Automatic
192.168.1.12        468b.ca4f.021c              Mar 01 2002 12:15 AM    Automatic
192.168.1.13        3d99.e041.32f7              Mar 01 2002 12:15 AM    Automatic
192.168.1.14        3188.b12a.befd              Mar 01 2002 12:15 AM    Automatic
192.168.1.15        f366.8428.bab5              Mar 01 2002 12:15 AM    Automatic
192.168.1.16        c59b.c116.74cd              Mar 01 2002 12:15 AM    Automatic
192.168.1.17        cd7c.5637.8c02              Mar 01 2002 12:15 AM    Automatic
192.168.1.18        fb86.c56a.dbed              Mar 01 2002 12:15 AM    Automatic
192.168.1.19        280a.1814.7a20              Mar 01 2002 12:15 AM    Automatic
192.168.1.20        b0fd.c701.8a1a              Mar 01 2002 12:15 AM    Automatic
192.168.1.21        d27e.bd55.04f9              Mar 01 2002 12:15 AM    Automatic
192.168.1.22        c784.eb5d.2087              Mar 01 2002 12:15 AM    Automatic
192.168.1.23        b69f.2e23.d0fc              Mar 01 2002 12:15 AM    Automatic
192.168.1.24        2ac1.8c53.d270              Mar 01 2002 12:15 AM    Automatic
192.168.1.25        a384.5019.cd79              Mar 01 2002 12:15 AM    Automatic
192.168.1.26        7ad4.9407.51b4              Mar 01 2002 12:15 AM    Automatic
192.168.1.27        0913.b277.1fb7              Mar 01 2002 12:15 AM    Automatic
192.168.1.28        aa9a.a935.d8e5              Mar 01 2002 12:15 AM    Automatic
192.168.1.29        190c.3922.3783              Mar 01 2002 12:15 AM    Automatic
192.168.1.30        3f50.5813.cabd              Mar 01 2002 12:15 AM    Automatic
192.168.1.31        715b.805d.1e16              Mar 01 2002 12:15 AM    Automatic
192.168.1.32        3cf6.0215.14ed              Mar 01 2002 12:15 AM    Automatic
192.168.1.33        eadc.bf3b.00fd              Mar 01 2002 12:15 AM    Automatic
192.168.1.34        70b2.8028.eb36              Mar 01 2002 12:15 AM    Automatic
192.168.1.35        646c.1631.68da              Mar 01 2002 12:15 AM    Automatic
192.168.1.36        ebe5.896b.0af2              Mar 01 2002 12:15 AM    Automatic
192.168.1.37        2f9c.3e37.27b4              Mar 01 2002 12:15 AM    Automatic
192.168.1.38        fe38.2d40.5396              Mar 01 2002 12:15 AM    Automatic
192.168.1.39        1616.e31a.e20d              Mar 01 2002 12:15 AM    Automatic
192.168.1.40        632d.c259.ecce              Mar 01 2002 12:16 AM    Automatic
192.168.1.41        d152.df34.3463              Mar 01 2002 12:16 AM    Automatic
192.168.1.42        1f3a.1f49.6b92              Mar 01 2002 12:16 AM    Automatic
192.168.1.43        9d61.b638.9353              Mar 01 2002 12:16 AM    Automatic
192.168.1.44        2012.2466.a6c8              Mar 01 2002 12:16 AM    Automatic
192.168.1.45        a6f7.235f.dbdb              Mar 01 2002 12:16 AM    Automatic
192.168.1.46        c4e0.ac25.bb8f              Mar 01 2002 12:16 AM    Automatic
192.168.1.47        634e.9623.b011              Mar 01 2002 12:16 AM    Automatic
 --More--
```

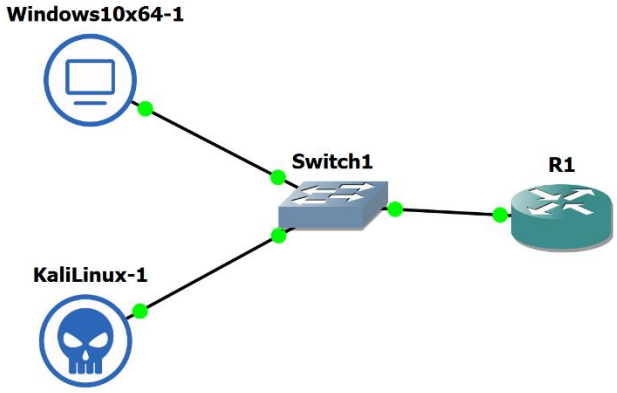
4.9 pav. Maršrutizatorius su daugybė klaidingų IP po atakos



4.10 pav. TShark duomenų rūšiavimas

4.3.3. *DHCP Rogue Server* ataka

Atakai atlikti buvo naudojama topologija (38 pav.) kurioje matomi du kompiuteriai – atakuojantis (KaliLinux-1) ir atakuojamas (Windows10x64-1), matomi maršrutizatorius ir komutatorius.



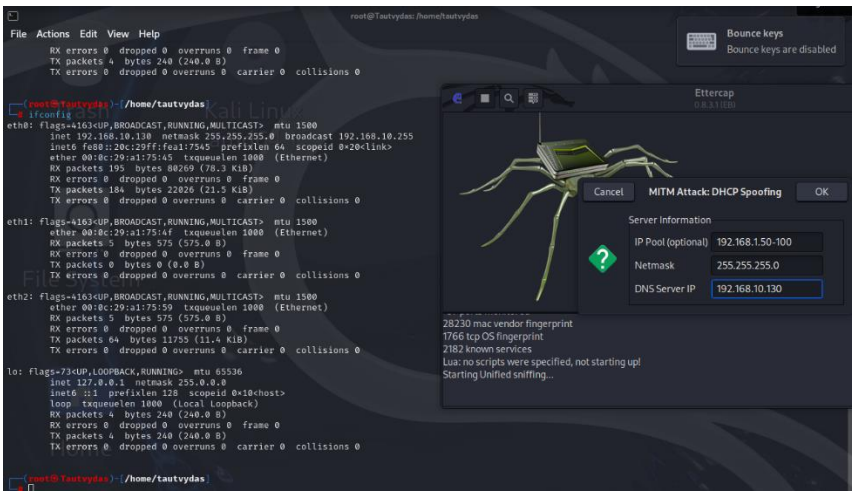
4.11 pav. GNS3 tinklo topologija

DHCP Rogue Server ataka yra kai asmuo ar įrenginys veikia kaip neteisėtas *DHCP* serveris tinkle. Jis skleidžia netinkamus *DHCP* adresus klientams, kurie gali būti nukreipti į kenksmingus arba netinkamus tinklo ryšio taškus. Tai leidžia užpuolikui stebėti, keisti ar netgi užkariauti klientų duomenis.

4.3.4. *DHCP Rogue Server* atakos simuliacijos eiga

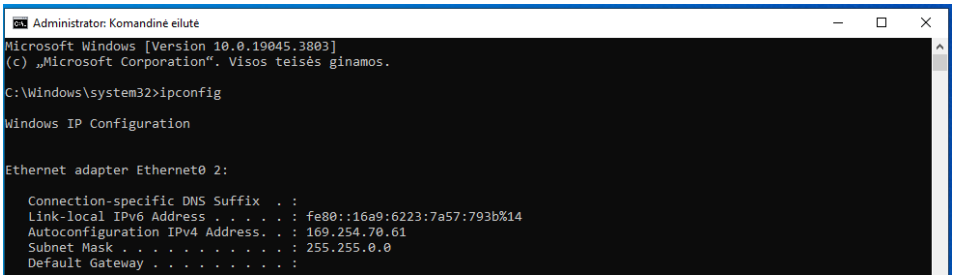
Su *GNS3* sukurtas tinklas (38 pav.), kuriam buvo naudojamas vienas „Switch“, keli kompiuteriai vienas atakuojantis, kitas kliento bei maršrutizatorius. Paleista *GNS3* aplinka ir pasijungta *Kali Linux*, pasirinkta programa *Ettercap (39 pav.)*, atidaryta programa ir pasirinkta primary interface pagal esantį tinklą. Paspaustas gaublys viršutiniame dešiniame kampe ir pasirinkta *DHCP spoofing*. Sukurta *DHCP Rogue Server*is. Pool‘e nustatytos ribos, šiuo atveju buvo 192.168.1.50-100, subnet mask 255.255.255.0 ir DNS serverio IP - buvo atakuojančio IP (38 pav.). Sukurtas *DHCP* serveris, tada atidaryta R1 konsolė ir išjungta *DHCP* service aplinkybė, jog būtų paprasčiau atlikti ataką, su komanda: „conf t“ > „no *DHCP* service.“ Tada pajungtas kliento kompiuteris ir atidaryta cmd arba *Windows* powershell, suvesta komanda: ipconfig /release po šios komandos vesta: ipconfig /renew (41 pav. 42 pav.). Po šių veiksmų matoma, jog naujas IP adresas yra tarp nustatytų pool ribų, o default gateway atakuojančio kompiuterio IP adresas. Prisijungta į

tinklą arba svetainę, kur reikia įvesti prisijungimo duomenis. *Ettercap* programoje matomi http svetainės duomenys bei prisijungimai. Stebėjimui naudota *WireShark* aplinka (43 pav.).

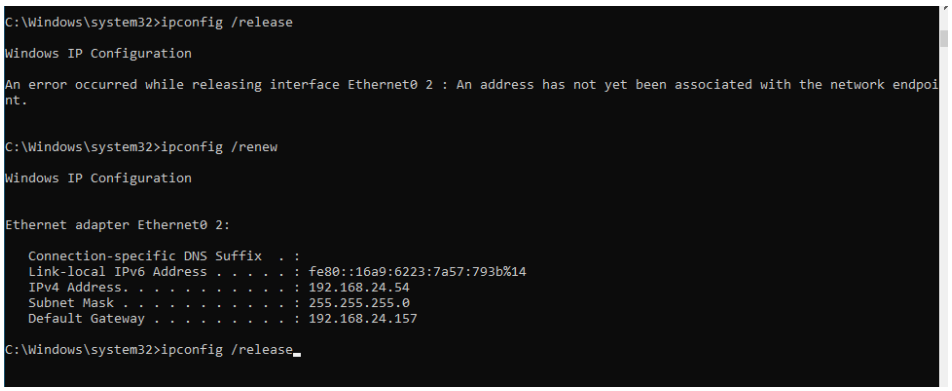


4.12 pav. "Ettercap" programos vaizdas

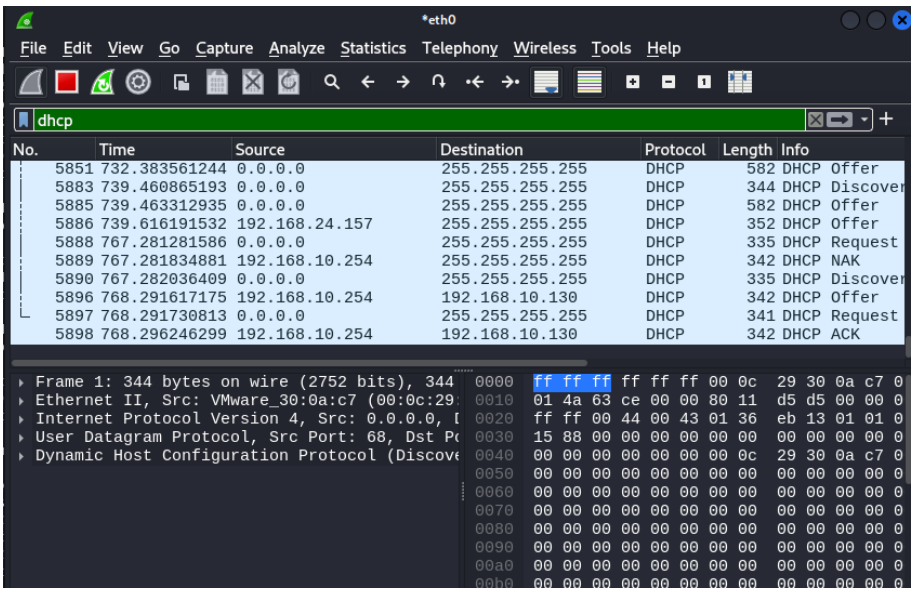
4.13 pav. Klaidingai siūlomas IP



4.14 pav. IP duomenys prieš ataką



4.15 pav. IP duomenys po atakos



4.16 pav. WireShark programa ir DORA paketų kelias

4.3.5. Apibendrinimas

Ataka *DHCP Starvation* pavyko, turėta sunkumų su R1 konfigūracija, tačiau atlikus išsamią analizę pavyko surasti sprendimą ir ištaisyti klaidas. *Kali Linux* platformoje *Yersinia* -G grafinė aplinka neveikė, todėl naudota *Yersinia* -I aplinka, tačiau tai nesutrukdė atlikti atakos ir papildomų rūpesčių nesukėlė. Duomenys surinkti ir išrūšiuoti. Kalbant apie sekančią ataką, problemų kilo daug daugiau - IP adresas prisiskyrė ir *DHCP Rogue Server*is buvo sukurtas, tačiau negalėjau prisijungti prie interneto atakuojamame kompiuteryje ir stebėti srauto per *WireShark*.

1 lentelė. Apibendrinimas

Scenarijus/ataka	Scenarijaus/atakos įgyvendinimas	Duomenų surinkimo įgyvendinimas	Pastabos
DHCP Starvation	Pavyko	Pavyko	*Yersinia* -G grafinis vaizdas neveikia kokybiškai ko pasekoje buvo naudota *Yersinia* -I aplinka ir dirbta su ja.
DHCP Rogue Server	Dalinai	Dalinai	Po komandos ipconfig /renew IP adresas prisiskyrė tačiau jungiantis prie interneto nebuvo galimybės stebėti kliento srauto kur ir ką klientas veikia, bei nebuvo galima stebėti slaptažodžių. Kilo problemų su eth adapteriais, nebuvo interneto.

4.3.6. Eksperimentinės dalies išvados

Eksperimentas parodė, kad tinklas yra pažeidžiamas *DHCP Starvation* atakai. R1 maršrutizatorius nebuvo tinkamai apsaugotas nuo šios atakos, o tai leido atakuotojui išgauti didelį skaičių IP adresų iš pool'o. Tinklo konfigūracijoje nustatytos neatsargios IP adresų ribos, kurios leido atakuotojui sėkmingai vykdyti ataką ir išsiųsti net 105 klaidingus IP adresus kuriuos gavo maršrutizatorius. Be to, atakuojantysis nebuvo tinkamai aptiktas ar sustabdytas. Siekiant apsaugoti tinklą nuo panašių atakų, svarbu tinkamai konfigūruoti *DHCP* serverį ir nustatyti saugumo priemones, pavyzdžiui, filtravimą ir IP adresų ribojimą. Taip pat būtina stebėti tinklo srautą ir reaguoti į neįprastą veiklą. Eksperimentas parodė ir koks svarbus įrankis *WireShark*, kuris padeda stebėti tinklo srautą.

DHCP Rogue Server ataka, kadangi po ipconfig /renew IP adresas prisiskyrė, tačiau nebuvo prisijungta prie interneto, tai rodo, kad *DHCP Rogue Server*is sėkmingai nustatytas ir kliento kompiuteris gavo naują IP adresą iš sukurto pool‘o ribų, tačiau DNS serverio nustatymai neteisingi arba tinklas nėra tinkamai maršrutizuotas, todėl nepasiektas interneto ryšys. Tai parodo, jog atakų atlikimas nėra labai lengvas ir paprastas.

Naudojama stebėjimo įranga veikė puikiai, *WireShark* galingas įrankis, kuris tikrai padeda rengiant atakas, duomenų srauto paketų generavimui ir duomenų rūšiavimui tinkama naudojama *TShark*, paprasta naudotis ir patogiai konfigūruojamos komandos. Visi surinkti duomenys galimi mašininio mokymo panaudojimui, tačiau gauti kiekiai yra per maži norint užtikrinti didelį efektyvumą, todėl reikėtu duomenų generuoti didesniais kiekiais.

IŠVADOS

1. Atlikta *DHCP* protokolo ir jo atakų literatūros analizė ir išsiaiškintos pagrindinės atakų rūšys, jų vykdymo procesai, etapai ir joms reikalingos naudojamos priemonės. Tai padėjo lengviau simuliuoti atakas simuliacinėje aplinkoje.
2. Atlikta analizė, įvertintos virtualios mašinos ir pasirinktos platformos su kuriomis atlikti simuliaciniai veiksmai ir atitinkamos *DHCP* protokolo atakos.
3. Suprojektuotas simuliacinis tinklas, sukurtos tinklo topologijos, kurios atitiko reikalavimus pasirinktoms atakoms atlikti.
4. Apžvelgti pagrindiniai veiksniai ir duomenų generavimo svarba mašininiam mokymuisi. Pastebėta, kad gautų duomenų kiekis yra per mažas ir reikėtu didesnio kiekio duomenų norint efektyviau pritaikyti duomenis mašininiam mokymui.
5. Atliktos *DHCP* protokolo atakos, pastebėta silpnos įrenginių vietos, nustatyta konfigūravimo pažeidžiamumai, surinkti duomenys. Pastebėta, kad esant neapsaugotam *DHCP* serveriui galima labai lengvai jį atakuoti ir siųsti klaidingus adresus bei gauti kliento duomenų informaciją.
6. Gauti rezultatai įvertinti, pateiktos rekomendacijos kaip apsisaugoti nuo tam tikrų atakų.
7. Pastebėta, kad *DHCP Starvation* atakos metu per 20s nuo atakos pradžios užpuolikui su *Yersinia* atakavimo programa pavyko išsiųsti daug klaidingų IP adresų ir 105 klaidingi adresai pasiekė savo tikslą ir užkimšo DHCP serverį. Nesant tinkamai apsaugai, galima daryti prielaidą jog, *DHCP* serverį kuris turi 254 IP adresų vietas galima užkimšti per apytiksliai 1min laiko.
8. Atlikus *DHCP Rogue server* ataką pastebėta, kad nesant tinkamai apsaugotam tinklui užpuolikas gali lengvai prijungti savo DHCP serverį ir klaidingai siųsti naujus IP adresus klientams, ir vėliau matyti visus jų prisijungimus, bei ką jie veikia ir kuo naudojasi internete.

LITERATŪRA IR KITI INFORMACIJOS ŠALTINIAI

1. A look at 30 key cyber crime statistics 2023 data update. Prieiga per internetą: https://www.thesslstore.com/blog/cyber-crime-statistics/(žiūrėta 2024m. vasario 17d.).
2. DHCP Rogue Server atakos. Dio Aditya Pradana,Ade Surya Budiman, 2020. Prieiga per internetą: https://ejournal.uin suka.ac.id/s aintek/ijid/articl e/view/2287 (žiūrėta 2024m. gegužės 15d.).
3. DHCP attacking tools: an analysis. Prieiga per internetą: https://link.springer.com (žiūrėta 2024m. vasario 10d.).
4. Hero Wintolo, Yuliani Indrianingsih, Wahyu Hamdani, Syafrudin Abdie. (2023).Descriptive Analysis and ANOVA Test with File Sending on Computer Networks Attacked with Rogue‘s Dynamic Host Configuration Protocol (DHCP). Prieiga per internetą: https://eprints.uad.ac.id/43224/1/13- (žiūrėta 2024m. vasario 15d.).
5. Hero Wintolo, Yuliani Indrianingsih, Wahyu Hamdani, Syafrudin Abdie. (2023). Descriptive Analysis and ANOVA Test with File Sending on Computer Networks Attacked with Rogue‘s Dynamic Host Configuration Protocol (DHCP). Prieiga per internetą: https://eprints.uad.ac.id/43224/1/13- (žiūrėta 2024m. vasario 15d.).
6. Detecting stealth DHCP Starvation attack using machine learning approach. Prieiga per internetą: https://link.springer.com/article/10.1007/s11416-017-0310-x (žiūrėta 2024m. vasario 18d.).
7. Edgar, T., W. & Manz, D., O. (2017). Research Methods for Cyber Security. Syngress. Prieiga per internetą:https://www.sciencedirect.com (žiūrėta 2024m. gegužės 17d.).
8. Nuhu Abdulhafiz A., Echobu Faith O. and Olanrewaju Oyenike M (2020). FUDMA Journal of Sciences (FJS). Prieiga per internetą: https://fjs.fudutsinma.edu.ng (žiūrėta 2024m. vasario 18d.).
9. GNS3. (n.d.). Getting Started with GNS3. Prieiga per internetą: https://docs.GNS3.com/docs/ (žiūrėta 2024m. balandžio 15d.).
10. Gihan, K. (2021). DHCP Starvation Attack using Python. Medium. Prieiga per internetą: https://kavigihan.medium.com/DHCP-starvation-attack-using-python-ab2f49c2d558 (žiūrėta 2024m. sausio 28d.).
11. Tamsir Ariyadi, Aidil NurRiyansyah, M. Agung, M. Alzi Ikrar (2023) Jurnal Ilmiah Informatika. Prieiga per internetą: https://ejournal.upbatam.ac.id/index.php/jif/article/view/7162/3105(žiūrėta 2024m. sausio 28d.).
12. Kali Linux. (n.d.). Kali Docs. Prieiga per internetą: https://www.kali.org/docs/ (žiūrėta 2024m. gegužė 8d.).

13. Q1 2023 Cyber attacks statistics. Prieiga per internetą: https://www.hackmageddon.com (žiūrėta 2024m. sausio 20d.).
14. Q2 2023 DDoS attacks statistics and overview. Prieiga per internetą: https://qratorlabs.medium.com (žiūrėta 2024m. vasario 15d.).
15. TShark. (n.d.). TShark(1) Manual Page. Prieiga per internetą: https://www.WireShark.org (žiūrėta 2024m. vasario 22d.).
16. Undag, E (2019). Attack a network by using a rogue DHCP server. Medium. Prieiga per internetą: https://medium.com/tech-jobs-academy/attack-a-network-by-using-a-rogue-DHCP-server-8c8acea315ab (žiūrėta 2024m. balandžio 20d.).
17. VMware. (n.d.). Documentation. Prieiga per internetą: https://docs.vmware.com/ (žiūrėta 2024m. balandžio 20d.).
18. WireShark. (n.d.). WireShark User's Guide. Prieiga per internetą: https://www.WireShark.org/docs/wsug_html_chunked/ (žiūrėta 2024m. vasario 20d.).
19. Yersinia. Prieiga per internetą: https://books.google.lt/books (žiūrėta 2024m. gegužės 15d.)
20. Yildiran Yilmaz, Selim Buyrukoglu, (2023). Development and Evaluation of Ensemble Learning Models for Detection of Distributed Denial-of-Service Attacks in Internet of Things Prieiga per internetą: https://dergipark.org. (žiūrėta 2024m. gegužės 18d.).