KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

Lukas Gaidys

Pramoninio kompiuterinio tinklo įsilaužimų aptikimo sistemos modelio sudarymas ir tyrimas

Baigiamasis magistro darbas

Vadovas
dr. Dangis Rimkus

KAUNAS, 2017

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Pramoninio kompiuterinio tinklo įsilaužimų aptikimo sistemos modelio sudarymas ir tyrimas

Baigiamasis magistro darbas
Informacijos ir informacinių technologijų sauga (kodas 621E10003)

Vadovas
(parašas) dr. Dangis Rimkus
(data)

Recenzentas
(parašas) doc. Agnius Liutkevičius
(data)

Projektą atliko
(parašas) Lukas Gaidys
(data)

KAUNAS, 2017

KAUNO TECHNOLOGIJOS UNIVERSITETAS
Informatikos fakultetas
(Fakultetas)
Lukas Gaidys
(Studento vardas, pavardė)
"Informacijos ir informacinių technologijų sauga" (621E10003)
(Studijų programos pavadinimas, kodas)

„Pramoninio kompiuterinio tinklo įsilaužimų aptikimo sistemos modelio sudarymas ir tyrimas“

AKADEMINIO SĄŽININGUMO DEKLARACIJA

2017 m. gegužės 15 d.
Kaunas

Patvirtinu, kad mano **Luko Gaidžio** baigiamasis projektas tema „Pramoninio kompiuterinio tinklo įsilaužimų aptikimo sistemos modelio sudarymas ir tyrimas“ yra parašytas visiškai savarankiškai, o visi pateikti duomenys ar tyrimų rezultatai yra teisingi ir gauti sąžiningai. Šiame darbe nei viena dalis nėra plagijuota nuo jokių spausdintinių ar internetinių šaltinių, visos kitų šaltinių tiesioginės ir netiesioginės citatos nurodytos literatūros nuorodose. Įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs.

Aš suprantu, kad išaiškėjus nesąžiningumo faktui, man bus taikomos nuobaudos, remiantis Kauno technologijos universitete galiojančia tvarka.

(vardą ir pavardę įrašyti ranka) *(parašas)*

Gaidys, Lukas. „Pramoninio kompiuterinio tinklo įsilaužimų aptikimo sistemos modelio sudarymas ir tyrimas“. Magistro baigiamasis projektas / vadovas dr. Dangis Rimkus; Kauno technologijos universitetas, Informatikos fakultetas, Kompiuterių katedra.

Reikšminiai žodžiai: pramonės sistemos, tinklų saugumas, įsilaužimų aptikimas.

Kaunas, 2017. 60 p.

SANTRAUKA

Pramonės valdymo sistemos yra naudojamos elektros, vandens ir nuotekų, naftos ir gamtinių dujų, chemijos, transporto, farmacijos ir kituose pramonės sektoriuose. Kenkėjiški veiksmai pramonės valdymo sistemose turi didelį poveikį fiziniame pasaulyje: gali iškilti pavojus žmonių saugumui ir sveikatai, sukelti didelius neigiamus padarinius aplinkai, padaryti didelius finansinius nuostolius, didelę žalą valstybės ekonomikai. Atsiradus verslo poreikiui sujungti technologinius tinklus su korporatyviniais tinklais, šiuolaikinės pramonės valdymo sistemos tampa vis labiau pažeidžiamos, nes telekomunikacijų tinklų ir sistemų pažeidžiamumai kelia grėsmę pramoniniams tinklams ir sistemoms.

Šiame darbe nagrinėjami įsilaužimų aptikimo metodai ir jų pritaikymas pramoniniuose tinkluose. Atsižvelgiant į analizuotų metodų trūkumus, yra pasiūloma sistema, kuri galėtų aptikti įlaužimą pirminėse jo stadijose, kuomet bandoma analizuoti vidinį aukos tinklą. Eksperimentinėje dalyje siūlomo metodo pagrindu sukurtas prototipas buvo įvertintas, pateiktos pastabos ir rekomendacijos.

Gaidys, Lukas. *Development and Research of Intrusion Detection System Model for Industrial Computer Network*: *Master's* thesis in "Information and Information Technology Security" / supervisor assoc. prof. Dangis Rimkus. The Faculty of Informatics, Kaunas University of Technology.

Research area and field: Industrial computer network security.

Key words: industrial systems, network security, intrusion detection.

Kaunas, 2017. 60 p.

SUMMARY

Industrial control systems are used in electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical and other industries. Malicious activities in industrial control systems can have a large impact in the real word such as an increased risk to human safety and health, negative impact to the environment and economy, large financial loss. Modern industrial control systems are becoming more vulnerable, because business networks and industrial networks are becoming more interconnected. Therefore, standard information technology attacks and vulnerabilities are being exploited in industrial networks.

This work analyzes intrusion detection methods for industrial control networks. Based on found flaws a new system is proposed, which could detect early signs of intrusion, when the internal network is being mapped. A prototype for the proposed system is developed and analyzed.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

TERMINŲ IR SANTRUMPŲ ŽODYNAS

ICS - pramonės valdymo sistema (angl. *industrial control system*);

SCADA – priežiūros kontrolės ir duomenų įgijimo sistemos (angl. *supervisory control and data acquisition*);

DCS – paskirstyto valdymo sistemos(angl. *distributed control systems*);

PLC – programuojami loginiai valdikliai (angl. *programmable logic controllers*);

RTU – nutolę terminaliniai valdikliai(angl. *remote terminal unit*);

HMI – žmogaus ir mašinos sąsajų (angl. *human – machine interface);*

IT – informacinės technologijos;

IP – interneto protokolas;

LAN – vietinis kompiuterių tinklas (angl. *local area network*);

Zero day vulnerability – viešai nežinomas pažeidžiamumas;

VPN – virtualus privatus tinklo tunelis (angl. *Virtual Private Network*).

ĮVADAS

Pramonės valdymo sistemos pastaruoju metu įgijo IT saugumo tyrėjų dėmesį kaip kritinė infrastruktūra šiuolaikiniame pasaulyje. Pastarųjų metų incidentai parodė, kad kenkėjiški veiksmai pramonės valdymo sistemose turi didelį poveikį fiziniame pasaulyje: gali iškilti pavojus žmonių saugumui ir sveikatai, sukelti didelius neigiamus padarinius aplinkai, padaryti didelius finansinius nuostolius, didelę žalą valstybės ekonomikai.

Šiame darbe nagrinėjama problematika bei siūlomas sprendimas yra aktualūs pramonės sektorių įmonėms.

Darbo tikslas ir uždaviniai

Šio darbo tikslas yra sukurti sistemos modelį ir šio modelio pagrindu sukurti sistemos prototipą, skirtą aptikti įsilaužimą pramoniniame kompiuteriniame tinkle. Šiam tikslui pasiekti reikia atlikti tokius uždavinius:

- atlikti pramoninių kompiuterinių tinklų saugumo problemų analizę;
- išanalizuoti ir įvertinti esamus įsilaužimų aptikimo metodus ir sistemas pramoniniuose tinkluose;
- atsižvelgiant į analizės išvadas, sukurti įsilaužimų aptikimo sistemos modelį;
- sukurti prototipą, atlikti bandymus ir įvertinti gautus rezultatus.

Darbo struktūra

Dokumentą sudaro keturi pagrindiniai skyriai:

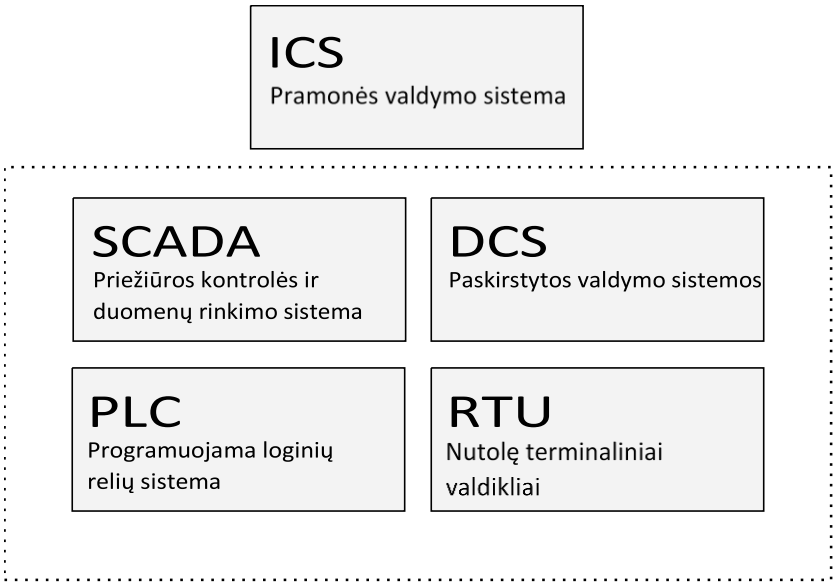
- **Pramonės valdymo sistemų saugumas**. Analizuojamos pramoninių tinklų grėsmės, pažeidžiamumai, aktualūs incidentai ir saugumo rekomendacijos;
- **Įsilaužimų aptikimo sistemų analizė.** Išanalizuojamos įsilaužimų aptikimo sistemos, jų veikimo principai ir pritaikomumas pramonės tinklams. Įvertinami kitų mokslinių darbų siūlomi metodai, pateikiamos pastabos;
- **Įsilaužimų aptikimo sistemos koncepcija ir modelis.** Atsižvelgiant į analizės išvadas, aprašomas ir argumentuojamas įsilaužimų aptikimo sistemos modelis, įvertinami jo privalumai ir trūkumai, aprašoma prototipo realizacija;
- **Tinklo žvalgybos aptikimo tyrimas.** Atliekamas siūlomos sistemos modelio tyrimas vykdant tinklo žvalgybą bandomoje aplinkoje. Apibendrinami atliktų tyrimų rezultatai.

1. PRAMONĖS VALDYMO SISTEMŲ SAUGUMAS

Pramonės valdymo sistema (angl. *industrial control system,* ICS) yra bendras terminas, kuris apima kelias kontrolės sistemų ir įrenginių rūšis [1]:

- priežiūros kontrolės ir duomenų įgijimo (angl. *supervisory control and data acquisition,* SCADA) sistemos;
- paskirstyto valdymo sistemos (angl. *distributed control systems,* DCS);
- nutolę konfigūracijos įrenginiai, pavyzdžiui, programuojami loginiai valdikliai (angl. p*rogrammable logic controllers,* PLC).

Šios sistemos ir įrenginiai (1.1 pav.) dažniausiai naudojami pramonės sektoriuose ir ypatingos svarbos infrastruktūros objektuose. Pramonės valdymo sistemos yra naudojamos elektros, vandens ir nuotekų, naftos ir gamtinių dujų, chemijos, transporto, farmacijos ir kituose pramonės sektoriuose. Šios kontrolės sistemos pasaulyje dažniausiai priskiriamos prie ypatingos svarbos infrastruktūros objektų. Sparčiai tobulėjant technologijoms, vis didesnę įtaką pramonėje daro telekomunikacijų tinklų saugumas [1].

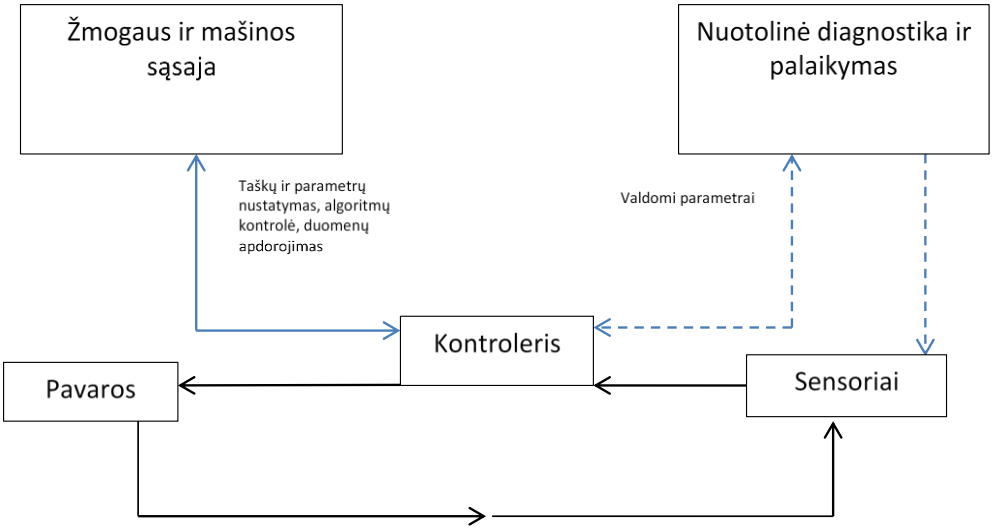


1.1 pav. Pramonės valdymo sistemų komponentai

1.1. Pramonės valdymo sistemų dalys

Tipinė pramonės valdymo sistema susideda iš kelių lygių kontrolės ir procesų kilpų, žmogaus ir mašinos sąsajų (angl. *human – machine interface,* HMI) bei nuotolinės diagnostikos sistemų (2 pav.). Dažniausiai šios kilpos yra sugrupuotos į pakopas, kuriose vienos priklauso nuo kitų. Stebėtojų lygio kilpos ir žemesnio lygio kilpos veikia nepertraukiamai, kurių proceso trukmė ir darbo ciklas svyruoja

nuo milisekundžių iki minučių. Bet kurio ciklo pertraukimas, sustabdymas arba piktavališkas modifikavimas gali sukelti kritinę situaciją [1].



1.2 pav. Pramonės sistemų valdymo procesai

1.1.1. Priežiūros kontrolės ir duomenų rinkimo sistema (SCADA)

SCADA yra ypatingai paskirstytos sistemos, naudojamos kontroliuoti geografiškai nutolusius įrenginius ir pramonines sistemas, kurios dažniausiai yra įrengtos labai didelėje teritorijoje [1]. SCADA valdymo centras telekomunikacijų tinklais atlieka centralizuotą lauko įrenginių, įskaitant signalizacijos ir būsenos duomenų apdorojimą, priežiūrą ir kontrolę. Apdorojus gautą informaciją iš nutolusių stočių, automatiniu arba rankiniu būdu gali būti nusiųstos atitinkamos komandos į nuotolinės kontrolės įtaisus, kurie dažnai vadinami lauko įrenginiais (angl. *field device*). Šie įrenginiai atlieka svarbias operacijas, tokias kaip vožtuvų atidarymas ir uždarymas, jungiklių valdymas, duomenų rinkimas, signalizavimas ir t.t.

1.1.2. Programuojama loginių valdiklių sistema (PLC)

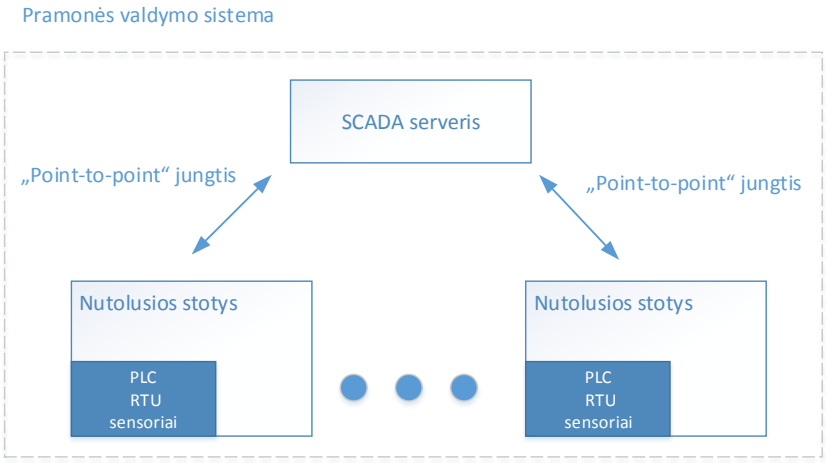
PLC yra dažnai naudojama pramonės kontrolės sistemose ir atlieka tam tikras, iš anksto apibrėžtas kontrolės sekas. Todėl PLC galima vadinti kaip specializuotus kompiuterius. Priklausomai nuo gamintojų, jie gali būti labiau atsparūs žemai arba aukštai temperatūrai, įvairiems aplinkos veiksniams ir gali būti naudojami tose vietose, kurios yra netinkamos standartinės paskirties kompiuterinei įrangai [1].

1.1.3. Nuotoliniai terminaliniai valdikliai (RTU)

Tiek RTU, tiek PLC paskirtis ir panaudojimo atvejai ICS yra panašūs. Lyginant su PLC, RTU suteikia daugiau duomenų valdymo ir apdorojimo galimybių, ją galima lengvai išplėsti papildomais moduliais [1].

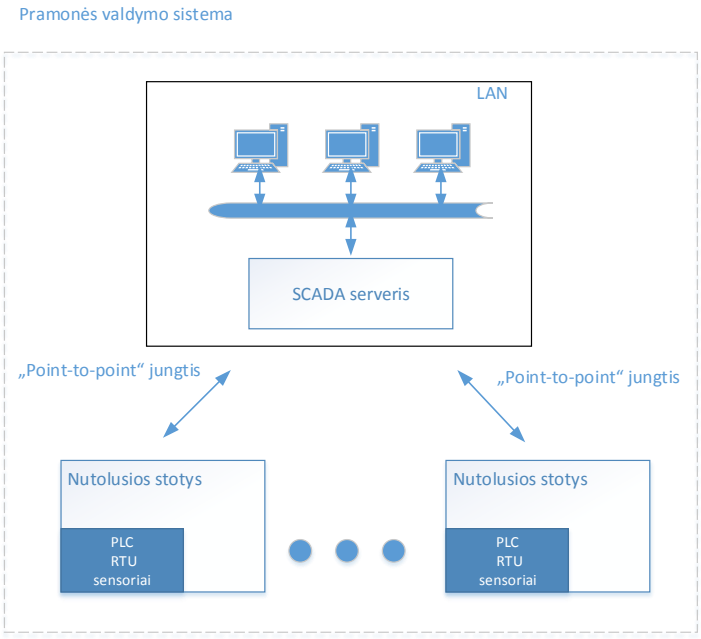
1.2. Pramonės valdymo sistemų architektūros kaita

Per pastaruosius kelis dešimtmečius ICS architektūra keitėsi [2]. Pirmos kartos ICS architektūra buvo vadinama monolitine (1.3 pav.). Kiekvienas PLC ar RTU buvo sujungtas su SCADA serveriu per „taškas į taškas“ (angl. *point-to-point*) jungtį. Be to, komunikacijoms buvo naudojami patentuoti (angl. *proprietary*) protokolai.



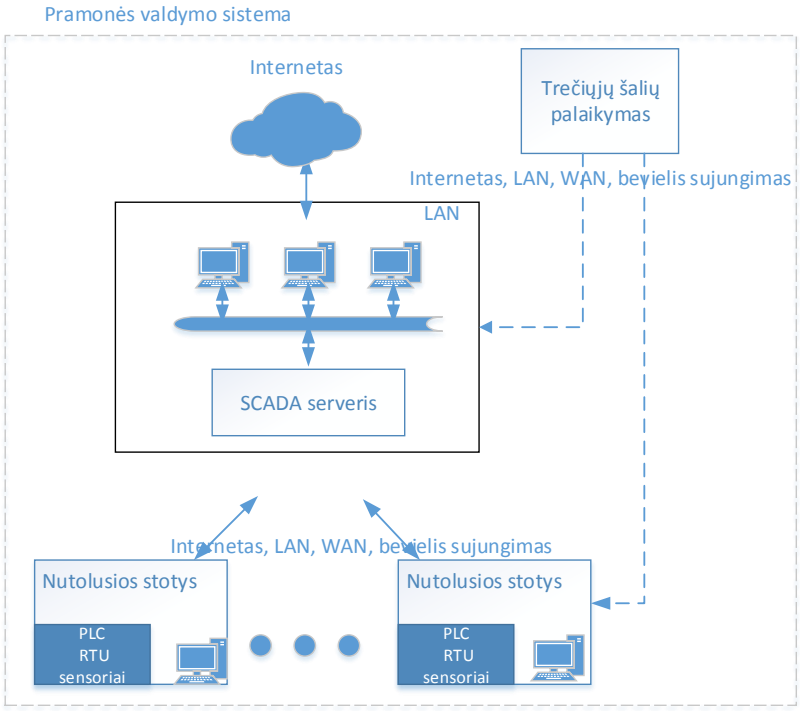
1.3 pav. Pirmos kartos ICS architektūra

Antros kartos ICS architektūra (1.4 pav.), dar vadinama paskirstyta ICS, panaudojo vietinio kompiuterių tinklo (angl. *local area network*, LAN) technologijas [2]. Tai uždaras tinklas, aptarnaujantis nedidelėje teritorijoje esančius vienos organizacijos įrenginius, tarpusavyje sujungtus telefoninio, varinio arba optinio kabelio ryšio kanalais. Lyginant su monolitine architektūra, bendrosios paskirties kompiuteriai kontroliuoja ir prižiūri nuotolines stotis per SCADA serverį.



1.4 pav. Antros kartos ICS architektūra

Trečios ir dabartinės kartos ICS architektūra (1.5 pav.) yra vadinama tinkline (angl. *networked*) [2]. Siekiant išplėsti SCADA funkcionalumą, supaprastinti migracijos ir diegimo darbus, tokiai architektūrai yra būdingas kompiuterių su tipinėmis operacijų sistemomis naudojimas, komunikacijos per standartinį TCP/IP protokolą, naudojami kiti telekomunikacijų standartiniai protokolai. SCADA sistemų gamintojai, siekdami palengvinti stebėsenos, priežiūros ir įrangos atnaujinimo darbus, vis dažniau į savo įrangą integruoja grafinę sąsają. Per tokia sąsają operatoriai gali lengvai stebėti bendrą sistemos būseną, greičiau reaguoti į incidentus, gamybos procesų pokyčius, greičiau aptikti pažeidimus, gedimus ir juos šalinti. Visa tai padeda užtikrinti nepertraukiamą gamybos procesą.



1.5 pav. Trečios kartos ICS architektūra

1.3. ICS ir IT skirtumai

Iš pradžių ICS turėjo mažai panašumų su tradicinėmis informacinių technologijų (IT) sistemomis, nes ICS buvo izoliuotos, naudojančios patentuotus (angl. *proprietary*) kontrolės protokolus ir specializuotą techninę bei programinę įrangą. Plačiai paplitę, mažų kaštų interneto protokolo (IP) įrenginiai dabar keičia patentuotus sprendimus, tačiau kartu didina ir kibernetinio pažeidžiamumo riziką [3].

Kuriant šiuolaikines ICS, vis labiau darosi aktuali ICS tiesioginė sąsaja su korporatyvinėmis ir verslo sistemomis. Tokia integracija sukuria naujas IT galimybes, tačiau tokiu būtu ICS tampa sistemų dalimi, turinčių sąsają su pasauliniu telekomunikacijų tinklu. Tokie sprendimai neišvengiamai verčia didinti šių sistemų apsaugą [3].

Nors daugiausia saugumo sprendimai yra kuriami tipinėms IT sistemoms ir infrastuktūrai, tačiau dažnu atveju papildomi saugumo sprendimai yra reikalingi ir ICS. Lyginant tradicines informacijos apdorojimo sistemas ir ICS, tam tikros techninės savybės yra panašios, tačiau ICS turi savybių, kurios skiriasi nuo tradicinių IT sistemų. Daugelis šių skirtumų kyla iš to, kad veiksmai pramonės valdymo sistemose turi didesnį poveikį fiziniame pasaulyje: gali iškilti pavojus žmonių saugumui ir sveikatai, dideli neigiami padariniai aplinkai, dideli finansiniai nuostoliai, didelė žala valstybės ekonomikai, saugomoms valstybės paslaptims ir pan. Todėl ICS yra keliami dideli našumo, patikimumo ir saugumo reikalavimai [4].

IT ir ICS reikalavimų skirtumai parodyti 1.1 lentelėje.

1.1 lentelė IT ir ICS reikalavimų skirtumai **[1]**

Kategorija	Tipinės informacinių technologijų sistemos	Pramonės valdymo sistemos
Našumo reikalavimai	- ne visada reikalauja realaus laiko; - atsakymai turi būti nuoseklūs; - aukšto pralaidumo reikalavimai; - didelis vėlavimas gali būti priimtinas.	- reikalingas realaus laiko našumas; - atsakymai jautrūs laikui; - vidutinis pralaidumas yra pakankamas; - didelis vėlavimas ir trikdžiai nepriimtini.
Pasiekiamumo reikalavimai	- sistemų perkrovimai yra priimtini; - prieinamumo trikdžiai dažnai gali būti toleruojami, atsižvelgiant į sistemos veiklos reikalavimus.	- sistemų perkrovimai dažniausiai yra nepriimtini; - pasiekiamumo reikalavimai gali reikalauti atsarginių sistemų buvimo; - veikimo nutraukimai turi būti planuojami iš anksto.
Rizikų valdymo reikalavimai	- pirmoje vietoje dėmesys skiriamas duomenų konfidencialumui ir vientisumui; - avarijų toleravimas yra mažiau svarbus, trumpalaikis pasiekiamumo nutraukimas nėra pagrindinė rizika; - pagrindinis rizikų poveikis yra verslo operacijų vėlavimas.	- pirmiausia dėmesys skiriamas žmonių saugumui; - avarijų toleravimas yra esminis tikslas – net ir trumpalaikis pasiekiamumo nutraukimas gali būti kritiškas; - pagrindinis rizikų poveikis yra iškeltos grėsmės žmonių gyvybei, aplinkai ir valstybės saugumui.

Saugumo tikslai	- pagrindinis tikslas yra apsaugoti IT turtą ir informaciją, kuri yra saugoma arba perduodama.	- pagrindinis tikslas yra apsaugoti sistemas.
Sistemos	- sistemos kuriamos standartinių operacijų sistemų pagrindu; - atnaujinimai vykdomi panaudojant automatinius atnaujinimo įrankius.	- sistemos dažniausiai susideda iš patentuotos programinės įrangos, dažniausiai be jokių įdiegtų saugumo komponentų; - atnaujinimai vykdomi labai kruopščiai, dažniausiai nenaudojant automatinius atnaujinimo įrankius.
Resursų plėtra	- sistemos turi pakankamai resursų, kad palaikytų papildomus trečiųjų šalių saugumo sprendimus.	- sistemos dažniausiai neturi pakankamai resursų, kad palaikytų papildomus trečiųjų šalių saugumo sprendimus.
Komunikacija	- naudojami standartiniai telekomunikacijų protokolai; - naudojamos tipinės IT tinklų praktikos.	- naudojama daug patentuotų ir uždarų telekomunikacijų protokolų; - naudojamos sudėtingos tinklų architektūros, kurios reikalauja aukštos kvalifikacijos specialistų jų priežiūrai.
Pokyčių valdymas	- programinės įrangos pokyčiai taikomi palankiu laiku. Dažniausiai tai diktuoja gerosios saugumo praktikos ir šios procedūros yra dažnai automatizuotos.	- programinė įranga turi būti kruopščiai patikrinta ir ištestuota, diegiama palaipsniui į sistemas, siekiant užtikrinti, kad būtų išlaikomas sistemų veikimo nepertraukiamumas, vientisumas ir kontrolė. Jei yra būtinas ICS sustabdymas, jis turi planuojamas iš anksto.
Palaikymas	- palaikymo galimybės iš skirtingų tiekėjų.	- palaikymas dažniausiai galimas tik iš sistemos gamintojo.
Komponentų gyvavimo ciklas	3-5 metai.	15-20 metų.
Komponentų pasiekiamumas	- komponentai yra lokalūs ir lengvai pasiekiami.	- komponentai yra izoliuoti, nutolę, reikalaujantys fizinių veiksmų juos pasiekti.

Apibendrinant galima teigti, kad dėl veiklos ir rizikų skirtumų tarp ICS ir standartinių IT sistemų, būtina kurti kitokias ICS kibernetinio saugumo ir nepertraukiamos veiklos užtikrinimo strategijas.

1.4. Incidentai pramoniniuose kompiuteriniuose tinkluose

1.4.1. „Stuxnet“ virusas

Vienas žinomiausių virusų-kirminų yra „Stuxnet“, aptiktas 2010 metais. Lyginant su įprastais virusais, „Stuxnet“ atakuoja kompiuterius su Windows operacijų sistema, kurie yra prijungti prie SCADA sistemos. Šių kompiuterių paskirtis prižiūrėti ir kontroliuoti PLC įrenginius, o pastarieji visą pramonės gamybos procesą. Virusas išnaudodavo keturias niekam nežinomas saugumo spragas (angl. *zero day vulnerability*) ir bandydavo aptikti ar kompiuteris yra prijungtas prie Siemens gamintojo „Simantic“ tipo įrenginių. Jei tokios sistemos ar įrenginiai nebūdavo aptikti, virusas žalos nepadarydavo. Aptikęs pramonės sistemas su Siemens gamintojo PLC, virusas apkrėsdavo įrenginį kenksmingu kodu ir pakeisdavo gamybos procesą [5].

Galima teigti, kad kenkėjiškai programai sukurti buvo skirta daug resursų, nes ji skirta tam tikrai specializuotai įrangai, kuri naudojama karinėje pramonėje, užkrėsti. Tokiais kompiuteriais valdomos centrifugos naudojamos karinėje pramonėje radioaktyvioms medžiagoms išskirti. 2010 m. Irane nepataisomai sugedo daug centrifugų. Ekspertai nustatė, kad kompiuteriniai virusai buvo problemų priežastis [6].

1.4.2. Kibernetinis išpuolis Ukrainoje

2015 metais prieš Ukrainos elektros perdavimo operatorius buvo įvykdytas organizuotas ir kryptingas kibernetinis puolimas, dėl kurio 230 tūkstančių vartotojų liko be elektros. Elektros tiekimas buvo atstatytas perėmus valdymą rankiniu būdu [7].

Įvykių eiliškumas:

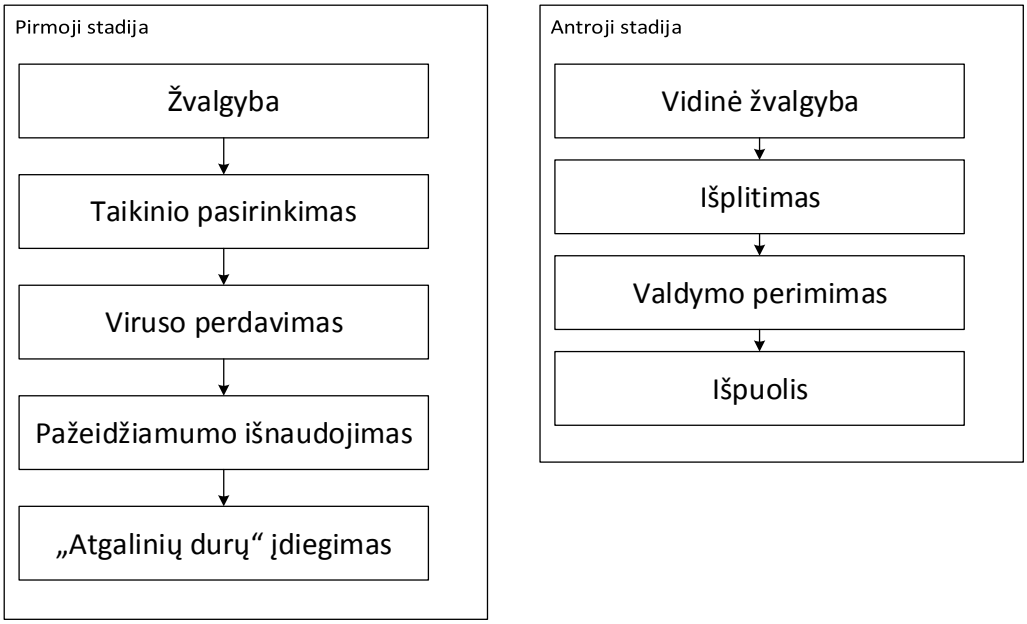
- įsiskverbta į SCADA sistemas;
- infekuotos kompiuterinės darbo vietos ir tarnybinės stotys;
- dispečeriams panaikinta galimybė valdyti sistemas;
- atjungtos elektros linijos;
- sunaikinta informacija ir pažeistos operacijų sistemos dispečerių darbo vietose ir tarnybinėse stotyse;
- naudojant DDOS tipo ataką paveiktos klientų aptarnavimo linijos.

Incidento priežastys:

Vadovaujantis SANS ICS analizės rezultatais [7], įsiskverbimui buvo panaudotas virusas „BlackEnergy“, siejamas su įsilaužėlių grupe „Sandstorm“ [8]. Virusas žinomas nuo 2007 metų, nuolat tobulinamas, jį naudoja nusikalstamos grupuotės ir kai kurių valstybių specialiosios tarnybos. Ukrainos atveju naudota vėliausia - BlackEnergy3 versija.

Ataką galima išskirstyti į dvi stadijas (1.6 pav.):

1. Įsilaužimas į vidinį tinklą;
2. Elektros valdymo sistemų sugadinimas.



1.6 pav. Ukrainos kibernetinio incidento įvykių eiliškumas

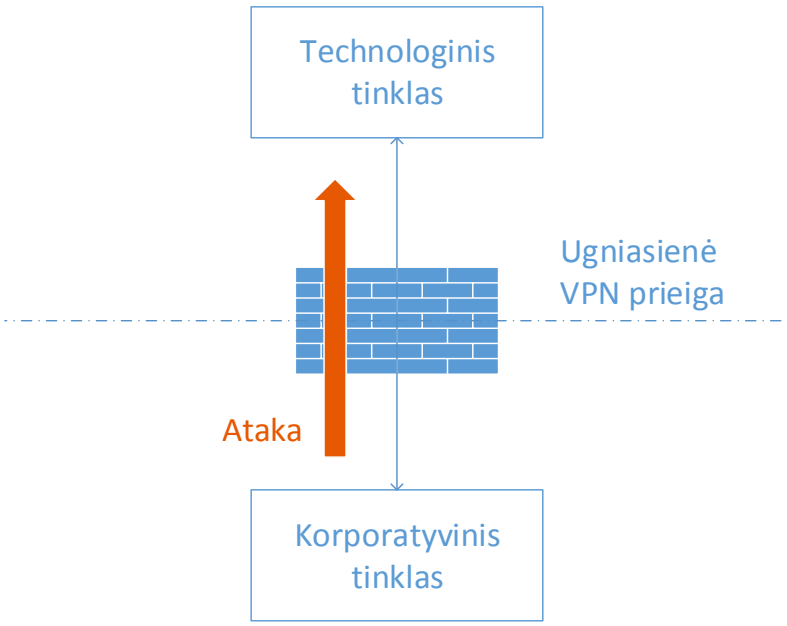
Virusas į Ukrainos bendrovių vidinius tinklus pateko naudojant „phishing“ tipo elektroninius laiškus, o kompiuterių kontrolę perėmė pasinaudojant neatnaujintomis „Microsoft Office“ programos versijomis [7].

Virusas sudarė galimybę įsilaužėliams:

- prisijungti prie vidinio tinklo nuotoliniu būdu;
- pasiekti tinklo viduje esančias valdymo sistemas;
- perimti elektros tinklo valdymą.

Virusas buvo panaudotas kaip „transportas“ įsilaužti ir gauti nuotolinę prieigą [7], o vėlesni destrukciniai veiksmai buvo atlikti rankiniu būdu. Tai galėjo atlikti asmenys, labai gerai išmanantys šias elektros valdymo sistemas. Tai vienas iš esminių skirtumų, lyginant su JAV priskiriamu „Stuxnet“ virusu, kuris destrukcinę veiklą atliko automatiškai, iš anksto užprogramuotu būdu.

Piktavaliai nuo įsilaužimo iki elektros atjungimo nepastebėti vidiniame tinkle buvo daugiau nei šešis mėnesius. Per tą laiką buvo pilnai perimtos SCADA sistemos. Reikia atkreipti dėmesį į tai, kad buvo įsilaužta į „Active Directory“ sistemą ir perimos darbuotojų paskyros. Perėmus paskyras, per vidinę VPN prieigą (1.7 pav.) buvo prisijungta prie technologinio tinko, nesukeliant jokių įtartinų veiksmų. Nors technologinis tinklas buvo logiškai izoliuotas ir atskirtas nuo korporatyvinio tinklo ugniasiene, piktavaliai pasinaudojo tomis pačios nuotolinės prieigos teisėmis kaip ir inžinieriai [7].



1.7 pav. Ukrainos incidento atakos kelias į technologinį tinklą

1.5. Pramonių sistemų grėsmės

Pirmos ir antros kartos ICS grėsmės kildavo lokaliai, nes sistemos neturėdavo tiesioginių jungčių su globaliais telekomunikacijų tinklais. Dabar šiuolaikinėms modernioms IT sistemoms reikalingas ne tik ryšys su korporatyvinio tinklo dalimi, bet ir nuotolinė prieiga prie korporatyvinio tinklo atsakingiems darbuotojams, tinklą aptarnaujančioms trečioms šalims. Korporatyviniame tinkle esančiai techniniai ir programinei įrangai grėsmės gali kilti iš daugelio šaltinių, įskaitant priešiškų valstybių, teroristinių grupuočių, nelojalių atsakingųjų darbuotojų, neprofesionalaus aptarnaujančio personalo, atsitiktinių klaidingų veiksmų [9].

1.5.1. Žinomos grėsmės ICS/SCADA sistemoms

2016 metais Europos Sąjungos tinklų ir informacijos apsaugos agentūra (toliau - ENISA) atliko pramonės tinklų grėsmių ir saugumo tyrimą [10]. Pagal jų rezultatus, kenksminga programinės įranga yra dažniausiai pasitaikančių pramonės tinklų kompromitacijos būdų.

1.2 lentelė ICS grėsmės **[10]**

Grėsmės	Aprašymas	Tikimybė	Reikšmė
Kenkėjiškos programos	Programinis kodas, skirtas atlikti nepageidaujamus ir neleistinus veiksmus be sistemos naudotojo sutikimo ir sukelti žalą, kompromituoti sistemą ar pavogti informaciją.	Labai aukšta	Didelė
Pažeidžiamumų išnaudojimai	Pažeidžiamumus išnaudojanti programa yra specialiai paruoštas	Vidutinė	Didelė

	programinis kodas, pasinaudojantis sistemos spraga ir siekiantis gauti prieigą prie sistemos. Tai yra viena iš didžiausių grėsmių ICS/SCADA tinklams. Tokią ataką gali surengti ir žemos kvalifikacijos asmuo (kenkėjišką programą jis gali paprasčiausiai nusipirkti), o tokios atakos žala gali būti didelė.		
APT (angl. Advanced Persistent Threats) atakos	Sunkiai aptinkamas sudėtingų metodų ir veiksmų, skirtų įsilaužimui į sistemas, rinkinys, kurį naudoja aukštą kvalifikaciją IT srityje turintys asmenys ar asmenų grupės prieš konkretų subjektą. Pagrindinis tikslas yra nepastebėtiems perimti kuo daugiau informacijos ar sistemų kontrolę, atsižvengiant į puolimo tikslus.	Žema	Didelė
Vidinės grėsmės	Darbuotojas, rangovas ar trečioji šalis piktybiškai pasinaudoja turima prieiga prie vidaus sistemų, tikslu pavogti duomenis, juos keisti ar neteisėtai gauti prieigą prie kitų sistemų.	Žema	Ypač didelė
Komunikacijų perėmimas	Neteisėtas informacijos ar valdymo komandų perėmimas realiu laiku ir jų panaudojimas kenkėjiškais tikslais.	Žema	Didelė
Duomenų srauto nutraukimas	Tyčinis arba netyčinis komunikacijų srauto nutraukimas.	Žema	Didelė/Ypač didelė
DDOS atakos	Tokios atakos vykdomos iš kelių sistemų, puolančių vieną įrenginį, siekiant, kad jis negalėtų aptarnauti tikrų užklausų. Jeigu ICS įrenginiai yra pažeidžiami, tokia ataka gali sutrigdyti gamybos procesą.	Žema	Vidutinė/Didelė
Informacijos nutekėjimas	Sąmoningas arba nesąmoningas jautrios informacijos atskleidimas ar perdavimas pašaliniams asmenims. Šio grėsmės reikšmė gali labai skirtis, priklausomai nuo nutekėjusių duomenų svarbos.	Žema	Vidutinė/Didelė

1.6. ICS pažeidžiamumai

Dauguma šiandien naudojamų pramonės valdymo sistemų buvo sukurtos palyginus seniai, kai dar neegzistavo vieši ir privatūs tinklai, namų kompiuterija (desktop computing) ir internetas nebuvo kasdieninė, plačiai naudojama komunikavimo priemonė. Šios sistemos buvo skirtos patenkinti

efektyvumo, patikimumo ir lankstumo reikalavimus, nebuvo atsižvelgiama į galimas kibernetines atakas. ICS pažeidžiamumai dažnai pasitaiko dėl nepilnos, netinkamos arba neegzistuojančios saugumo dokumentacijos, nesamos saugumo politikos, vidaus tvarkos procedūrų, operacijų sistemų ir įrangos trūkumų, netinkamos įrangos konfigūracijos ar prastos priežiūros, nekvalifikuoto personalo [11].

Kibernetinių incidentų skaičius pramoniniuose kompiuteriniuose tinkluose dramatiškai išaugo per pastaruosius metus. Tai iš dalies nulėmė didesnė IT ir ICS sistemų tarpusavio integracija ir korporatyvinių tinklų sujungimas su globaliais tinklais. Kompanijos Symantec duomenimis [12], 2015 metais buvo aptikti daugiau negu 135 pramoninių sistemų pažeidžiamumai, kai tuo tarpu 2014 metais jų buvo tik 35. Kompanijos Kaspersky Lab duomenimis [13], pusė visų 2015 metais viešai paskelbtų ICS pažeidžiamumų yra kritinio lygio. Šie skaičiai nėra dideli, tačiau tai nereiškia, kad ICS yra saugios. Tiesiog tyrėjams pramonės sistemos yra sunkiai prieinamos, nėra didelių investicijų į jų saugumo analizę.

Pažeidžiamumų skaičių pramoninėse sistemose nulemia [10]:

1. **Neegzistuojantis tinklo stebėsenos procesas**

Be aktyvaus ir nuolatinio tinklo stebėjimo yra sunku aptikti įtartiną veiklą, nustatyti galimas grėsmes ir operatyviai reaguoti į kibernetines atakas. įsilaižimo aptikimo sistemos (angl. *intrusion detection system*, IDS) ICS nėra taip dažnai naudojamos, kaip standartiniuose IT tinkluose. Be to, net jei yra IDS sprendimas, jis gali pilnai nepalaikyti ICS protokolų. Tai gali būti sprendžiama sukūrus anomalijų aptikimo sistemą. Ugniasienių ir antivirusinių programų naudojimas yra dažnesnis sprendimas, tačiau tai nėra universalus sprendimas ir neapima visų pavojų [10].

2. **Nepakankamas duomenų srautų supratimas**

Atsakingieji darbuotojai turi žinoti, kokie turi būti duomenų apsikeitimo srautai, naudojami protokolai, prievadai, kad būtų galima priimti pagrįstus ir teisingus sprendimus, kokios rūšies srautą leisti ir kuriuos srautus filtruoti. Pagal duomenų srautus būtina tinkamai segmentuoti tinklą [10].

3. **Vidinių tvarkų trūkumai**

Pažeidžiamumai ICS dažnai atsiranda dėl nepilnos, netinkamos arba neegzistuojančios saugumo dokumentacijos, netinkamų vidaus tvarkų ar procedūrų, tokių kaip [10]:

- neegzistuojantys saugumo mokymai;
- neegzistuojantys saugumo auditai;
- neegzistuojantys sistemos saugos nuostatai;
- neegzistuojančio sistemos veiklos atkūrimo plano;
- problemų spendimo gairių trūkumo.

4. **Neapmokytas personalas**

SCADA sistemų darbuotojų ir operatorių pareigos yra užtikrinti kontrolės sistemų veiklą. Pagrindiniai tikslai yra patikimumas ir prieinamumas, o tai neretai prieštarauja saugumui. Kadangi ICS darbuotojai dažniausiai sprendžia technines problemas, saugumo politikų kūrimui ir jų diegimui yra skiriamas nepakankamas dėmesys [10].

5. **Nesaugūs valdikliai ir įrenginiai**

Tam tikrų kategorijų nuotoliniai valdikliai ar įrenginiai turi žinomų saugumo spragų. Dažniausiai šie valdikliai ar įrenginiai skirti tam tikroms funkcijoms atlikti ir nepalaiko saugumo atnaujinimų ar saugumo sistemų juose įdiegimo. Dažnu atveju po įrengimo jie pamirštami. Tokia įranga lieka pažeidžiama daug metų [10].

6. **Nepakankamos ICS programinės įrangos saugos funkcijos**

SCADA programinė įranga paprastai turi ribotas saugumo galimybes ir jos ne visada įjungtos pagal nutylėjimą. Senesnėms ICS trūksta pagrindinių saugos funkcijų, arba jos yra minimalios. Todėl ICS naudotojams būtina reikalauti iš tiekėjų ar gamintojų ICS įrangos atnaujinimų [10].

7. **Įdiegta pašalinė programinė įrangą ICS kompiuteriuose**

Dėl silpnų saugos priemonių naudojimo, ICS kompiuteriuose gali nebūti patikros dėl pašalinės programinės įrangos įdiegimo [10].

8. **Autentifikavimo trūkumai**

Autentifikavimo funkcija yra skirta kontroliuoti leistiną ir neleistiną prieigą prie sistemų. Tačiau autentifikavimas gali būti lengvai pažeidžiamas jeigu nėra griežtai laikomasi slaptažodžių naudojimo tvarkos, t.y. sistema leidžia naudoti silpnus slaptažodžius, slaptažodžiai periodiškai nekeičiami, naudojamos bendros vartotojų paskyros, nėra vartotojų registravimo. Ypatingai seni įrenginiai turi silpnesnius autentifikavimo metodus. Konfidencialumas ir autentiškumas negali būti užtikrinamas naudojant atviro teksto transmisijas [10].

9. **Nesaugūs ICS protokolai**

Seniai sukurti pramonės valdymo sistemų protokolai neturi daugelio saugumo funkcijų:

- DNP3: šis protokolas pagal nutylėjimą neturi jokių saugumo priemonių ir gautos instrukcijos nėra patvirtinamos. Jei užpuolikas nusiųstų komandą, sistema ją vykdytų. Pavyzdžiui, komandos kodas 0x0D privers sistemą persikrauti, 0x13 kodas privers užkrauti naujus konfigūracijos parametrus [14];
- ICCP: ICCP protokolo standartinio įgyvendinimo sistemos turi plačiai žinomą buferio perpildymo spragą [15];
- Modbus: protokolas nepalaiko šifravimo ar pranešimų patvirtinimo, gautos instrukcijos yra besąlygiškai vykdomos. Pavyzdžiui, 0x05 kodas gali išjungti ar įjungti nuotolinius

pranešimus, 0x08 gali įjungti diagnostiką, 0x01 kodas gali perkrauti sistemą ir atkurti įvykių žurnalus [15];

- OPC: protokolo naudojama įrašymo funkcija suteikia galimybe įrašyti bet kokią reikšmę į bet kokį atminties adresą. Toks veiksmas gali leisti savavališko kodo vykdymą sistemoje (angl. arbitrary code execution) [15].

10. Tinklų atvirumas

Kuo labiau integruojami technologiniai ir korporatyviniai tinklai, tuo daugiau tampa pasiekiamos ir atviresnės ICS. Dėl verslo poreikių ir darbo patogumo prie integruotų tinklų yra įrengiamos nuotolinės prieigos, o tai sudaro sąlygas neteisėtai pasinaudoti šiomis galimybėmis [10].

11. Bevielės jungtys

Dėl geografiškai nutolusių sistemų, kai kuriais atvejais telekomunikacijai yra naudojami radijo ar mobilieji ryšiai. Priklausomai nuo įgyvendinimo, tokie komunikacijų būdai gali būti pažeidžiami tam tikromis atakomis [10].

1.7. Klasikinė atakos schema

Piktavaliai atakai dažniausiai ruošiasi iš anksto ir tam skiria nemažai laiko. Išpuolio veiksmus būtų galima suskirstyti į dvi grupes [16]:

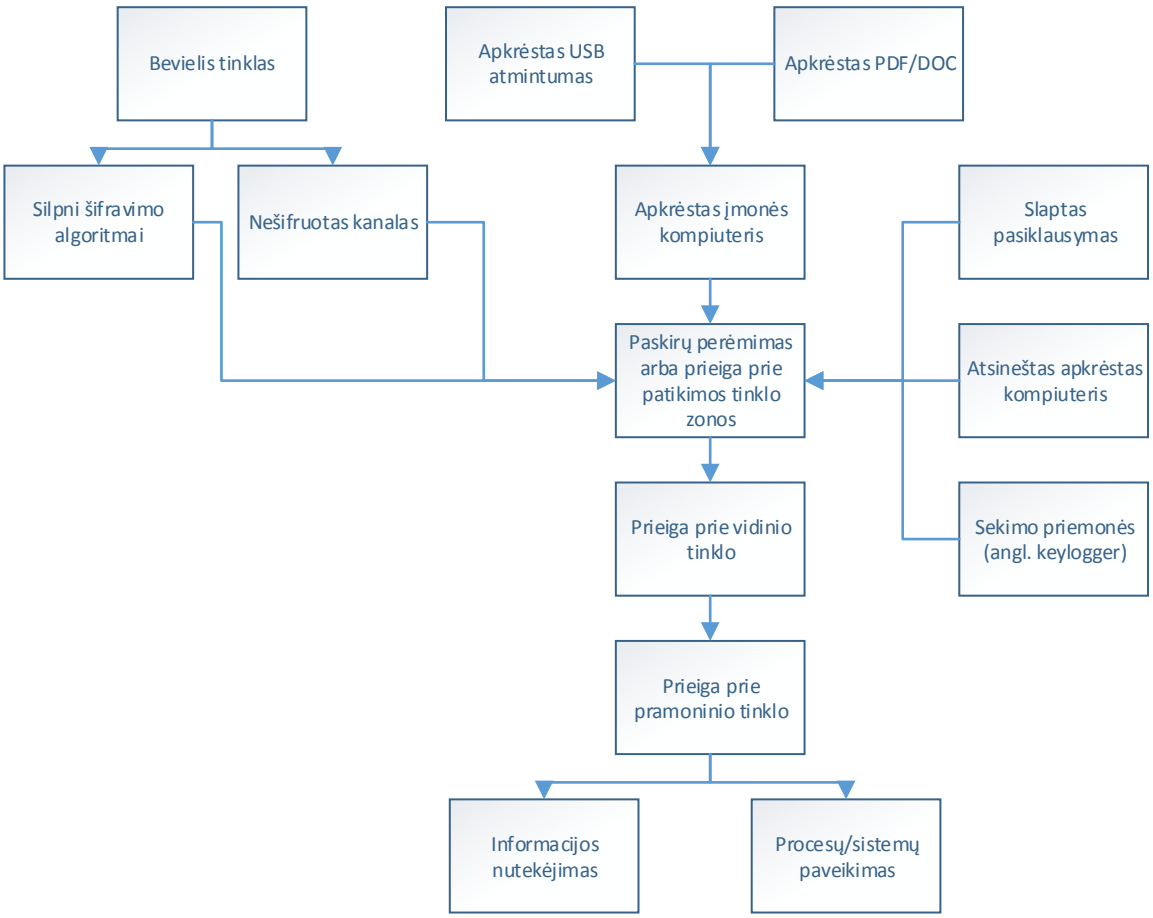
- Veiksmai išorėje;
- Veiksmai viduje.

Šie veiksmai turi skirtingus tikslus, tačiau jie yra būtini norint atlikti ataką sėkmingai. Ataka gali turėti skirtingus tikslus, pavyzdžiui, pavogti informaciją ar tiesiog sutrikdyti sistemų veikimą, padarant didelę žalą. Nusitaikęs į ICS, užpuolikas bandys pasiekti technologinį tinklą per tam tikrus tinklų sujungimo taškus.

Veiksmai išorėje

Pirmas etapas paprastai yra duomenų rinkimas, kai užpuolikas bando ieškoti naudingos informacijos apie auką iš įvairių šaltinių, pavyzdžiui, DNS įrašai, darbuotojų kontaktai, viešieji pirkimai ir pan. Taip pat per internetą yra tikrinami pasiekiami serverių adresai, atviri prievadai, aplikacijos, bandoma nustatyti kokios yra ugniasienės, galimi jų pažeidžiamumai, kokios naudojamos įsilaužimų aptikimo sistemos ir t.t [16].

Antrasis etapas yra jau konkreti ataka, kai užpuolikas bando išnaudoti pažeidžiamas vietas, tikslu pasiekti vidinį tinklą. 1.8 pav. pavaizduoti galimi įsilaužimo būdai ir eiga.



1.8 pav. Įsilaužimų būdai ir eiga

Veiksmai viduje

Pasiekęs vidinį tinklą, piktavalis visais įmanomais būdais stengiasi slėpti savo pėdsakus, kad liktų nepastebėtas ir galėtų toliau vykdyti savo neteisėtą veiklą, t.y. šalinami sistemų žurnaliniai įrašai apie prisijungimus, bandoma apsimesti kaip legalus vartotojas, perimamos jų paskyros ir pan. Patekęs į vidinį tinką piktavalis dažniausiai atlieka tokius veiksmus [16]:

- atlieka vidinio tinklo žvalgybą;
- išsiaiškina vidiniame tinkle veikiančius serverius ir apsaugos įrenginius bei įdiegtą programinę įrangą;
- išanalizuoja prisijungimo prie veikiančių sistemų galimybes ir būdus;
- toliau bando pasiekti kitas sistemas;
- sistemų paveikimas, žalos padarymas.

Vidinio tinklo žvalgyba

Šiame etape yra ieškoma aktyvių sistemų, vidinių apsaugos priemonių, pažeidžiamumų ar spragų, sudaroma vidinio tinklo architektūra.

Žvalgybos tipai ir tikslai [16]:

- prievadų skenavimas leidžia aptikti atvirus prievadus ir servisus;

- tinklo skenavimas leidžia identifikuoti aktyvius IP adresus tame tinkle ar potinklyje;
- pažeidžiamumo skenavimas leidžia aptikti žinomas programinės įrangos spragas.

Prievadų skenavimas – tai veiksmas, kurio metu identifikuojami atviri ir pasiekiami įrenginio prievadai. Prievadų analizės įrankiai leidžia programišiui sužinoti apie įrenginyje veikiančius servisus. Kiekvienas servisas ar programa įrenginyje yra susieti su konkrečiu prievado numeriu [16].

Tinklo skenavimas – tai veiksmas, kurio metu nustatomi tinkle esantys aktyvūs įrenginiai. Šie įrenginiai aptinkami pagal jų individualius IP adresus. Tinklo peržiūros įrankiai identifikuoja visus aktyvius ir į užklausas atsakančius įrenginius pagal jų IP adresus [16]. Šiam veiksmui gali būti naudojami tokie veiksmai:

- Ping yra ICMP echo užklausos ir ICMP echo atsakymo kombinacija. Ping iniciatorius siunčia ICMP echo užklausos žinutę į nurodytą IP adresą. Jei įrenginys veikia ir priima paketus, jis atsiunčia ICMP echo atsakymą [16];
- ARP protokolas veikia tik vietiniame tinkle ir pagal MAC adresus nustato IP adresus. Taip pat jis realizuoja užklausos / atsakymo šabloną. Jei norima sužinoti MAC adresą, kuris priklauso tam tikram IP, jis siunčia ARP užklausą į visą potinklį (angl. *broadcast*) ir, jeigu yra aktyvus įrenginys su tuo IP adresu, jis išsiunčia atsakymą su savo MAC adresu [16];

Pažeidžiamumo skenavimas – tai veiksmas, kurio metu identifikuojami programinės įrangos pažeidžiamumai. Pirmiausia pažeidžimumų ieškoma operacijų sistemoje, jos versijoje, atnaujinimuose, veikiančiuose servisuose. Toliau skenuojami kiti įrenginiai, pavyzdžiui demilitarizuotas (angl. demilitarized zone - DMZ) zonas aptarnaujantys įrenginiai, tose zonose esanti įranga [16].

Yra įvairių prievadų peržiūros metodų, kurie skiriasi sudėtingumu ir patikimumu. Dažniausiai naudojami metodai yra šie [16]:

- TCP *connect* - tai pats paprasčiausias TCP peržiūros metodas. *Connect*() sisteminis kreipinys naudojamas operacijų sistemos sujungimui su kiekvienu prievadu. Jei prievadas yra budėjimo režime, *connect*() bus sėkmingas, kitu atveju prievadas bus nepasiekiamas. Didžiausias minusas yra tas, kad tokio tipo peržiūra lengva aptikti ir perfiltruoti prievadus. Įrenginio žurnaliniai įrašai užfiksuos didelį kiekį susijungimų ir klaidų tų servisų, su kuriais buvo bandoma susijungti;
- TCP SYN *scanning* metodas dar vadinamas pusiau atviru skenavimu. Siunčiamas SYN paketas ir laukiama atsakymo. SYN|ACK atsakymas nurodo atvirą prievadą, o RST atsakymas yra uždaryto prievado indikatorius. Jei gaunamas SYN|ACK, iškart siunčiama RST tam, kad nutrauktų susijungimą;

- Kiti galimi metodai yra TCP NULL, FIN, Xmas skenavimas.

Išplitimas, perėjimas į kitas sistemas

Šiame etape įsilaužėliai pasiekia kitas sistemas išnaudodami rastus pažeidžiamumus ar saugumo spragas. Kadangi didesnis dėmesys saugumui yra skiriamas iš išorės pasiekiamoms sistemos, vidinės sistemos gali turėti apmaudžių saugumo spragų, tokių kaip numatytų paskyrų ir slaptažodžių naudojimas (1.6 skyrius). Tai ypač būdinga „interneto daiktų“ (angl. *internet of things*) įrenginiams, pavyzdžiui, IP kameros, bevielės prezentacijos įranga, išmanios durys ir pan.

Sistemų paveikimas, žalos sukėlimas

Veiksmai galutiniame etape priklauso nuo atakos tikslų ir galimybių. Ukrainos atveju (1.4.2 skyrius), galutinis tinklas buvo sutrikdyti sistemas ir nutraukti elektros tiekimą. Užpuolikai buvo įgavęs pilnas teises, todėl paveikti sistemas buvo nesudėtinga. Paskutinė ataka Ukrainos tinkle buvo įvykdyta labai greitai, operatoriams nespėjus laiku sureaguoti, nes įsilaužėliai turėjo prieigą prie daugelio sistemų ir tam buvo ruoštasi šešis mėnesius.

1.8. Saugumo rekomendacijos pramonės valdymo sistemoms

Veiksminga kibernetinio saugumo programa pramonės valdymo sistemoms turėtų taikyti strategiją, vadinamą "gynybos gilinimas" (angl. *defense-in-depth*), t.y. saugumas sluoksniais, pavyzdžiui, atakos ar gedimo poveikis bet kurioje vienoje sistemoje yra sumažintas iki minimumo [1].

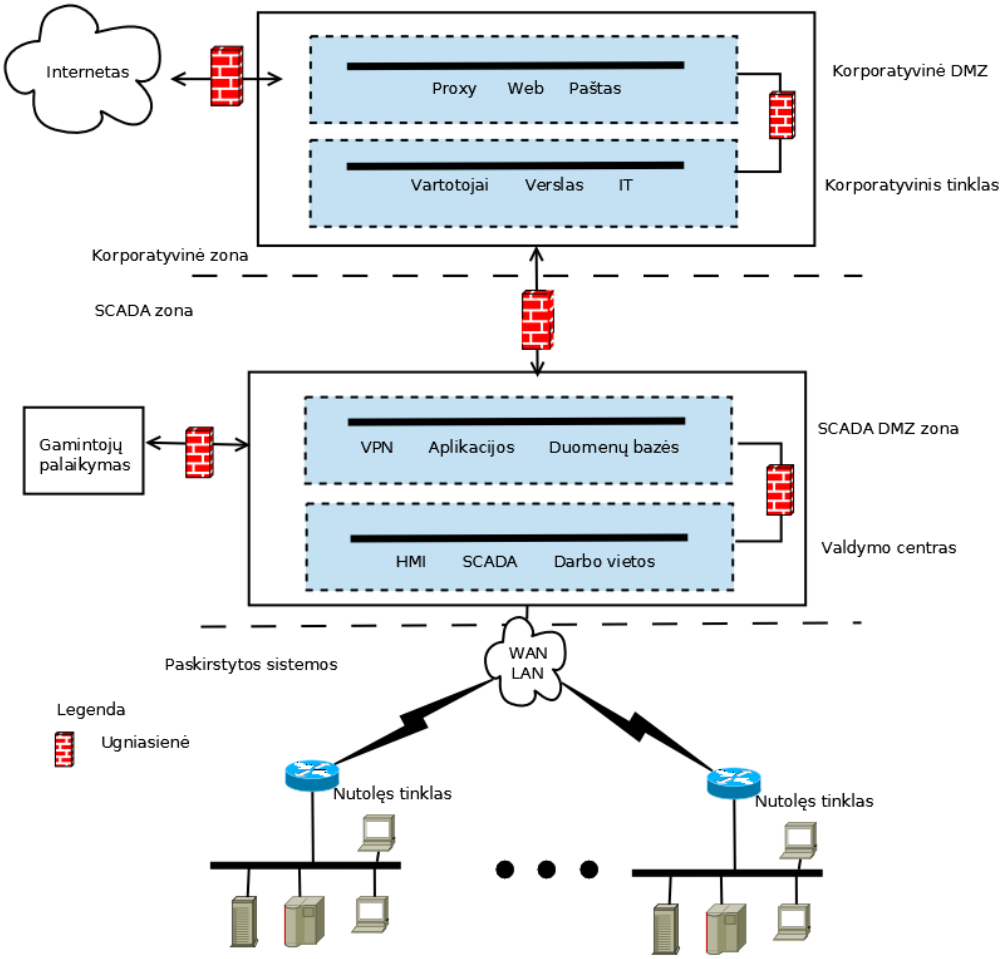
Pagrindiniai saugumo uždaviniai pramonės valdymo sistemoms turėtų būti šie:

Apriboti loginę prieigą prie ICS tinklo ir jo veiklos [1]. Tai įgyvendinama panaudojant demilitarizuotos zonos architektūrą su ugniasienėmis, siekiant apriboti tiesioginius tinklo srautus tarp technologinių ir korporatyvinių tinklų. Taip pat, naudoti skirtingus autentifikavimo būdus ICS ir korporatyviniams tinklams. ICS turėtų būti suskirstytas į kelias tinklo zonas, kur didžiausio kritiškumo srautai vyktų labiausiai apsaugotoje zonoje. Saugi tinklo architektūra parodyta 1.9 pav.

Apriboti fizinę prieigą prie ICS tinklo ir jo įrenginių [1]**.** Nesankcionuotos fizinės prieigos prie ICS komponentų gali sukelti rimtų sutrikimų sistemų funkcionavime. Kelios fizinės prieigos kontrolės priemonės turėtų būti naudojamos vienu metu, pavyzdžiui, spynos, kortelių nuskaitymo įrenginiai, kameros ir apsauga.

Apsaugoti individualius ICS komponentus nuo išnaudojimo [1]**.** Tai apima saugumo pataisų diegimą, nenaudojamų prievadų ir paslaugų išjungimą, vartotojų privilegijų apribojimą, tik būtinų atitinkamai rolei vykdyti. Saugumo kontrolės priemonių, tokių kaip antivirusinių ir failų integralumo patikros programinės įrangos panaudojimą, įsilaužimų aptikimo sistemų naudojimą.

Išlaikyti funkcionalumą nepalankiomis sąlygomis [1]**.** Tai reiškia, kad projektuojant ICS reikia atsižvelgti į galimus sistemų veikimo sutrikimus ir numatyti, kad kiekvienas kritinis komponentas turėtų atsarginį, pasiruošusį perimti pirmojo funkcijas. Papildomai reikia numatyti, kad gedimo atveju ICS komponentas nesukeltų papildomų srautų visoje sistemoje arba sukeltų progresuojančius įvykius (ang. Cascating events) kitur.



1.9 pav. Saugios pramoninio kompiuterinio tinklo architektūros pavyzdys

1.9. Apibendrinimas

Apibendrinant galima teigti, kad pramonės valdymo sistemų saugumas yra kritiškai svarbus, kadangi incidentai gali sukelti tiesioginę grėsmę žmonių saugumui, aplinkai ir valstybei. Šiuolaikinės ICS vis labiau pritaiko ir panaudoja standartizuotas IT technologijas, dėl to technologiniai tinklai tampa atviresni ir labiau pažeidžiami. ICS yra kuriamos be tinkamų saugumo priemonių, naudojami protokolai nepalaiko autentiškumo ir vientisumo tikrinimo, autorizacijos ir šifravimo. ICS apsauga turi būti kompleksinis sprendimas, apimantis saugią tinklo architektūrą, atskirų komponentų saugumą, įsilaužimų aptikimo sistemas, vidines tvarkas, personalo rengimo ir kvalifikacijos kėlimo politiką.

2. ĮSILAUŽIMŲ APTIKIMO SISTEMŲ ANALIZĖ

Šiuolaikinėse sistemose IDS poreikis auga, nes kuriamos vis sudėtingesnės sistemos, jose apdorojamos informacijos kiekiai didėja, informacijos aktualumas darosi vis svarbesnis.

2.1. Įsilaužimų aptikimo sistemų tipai

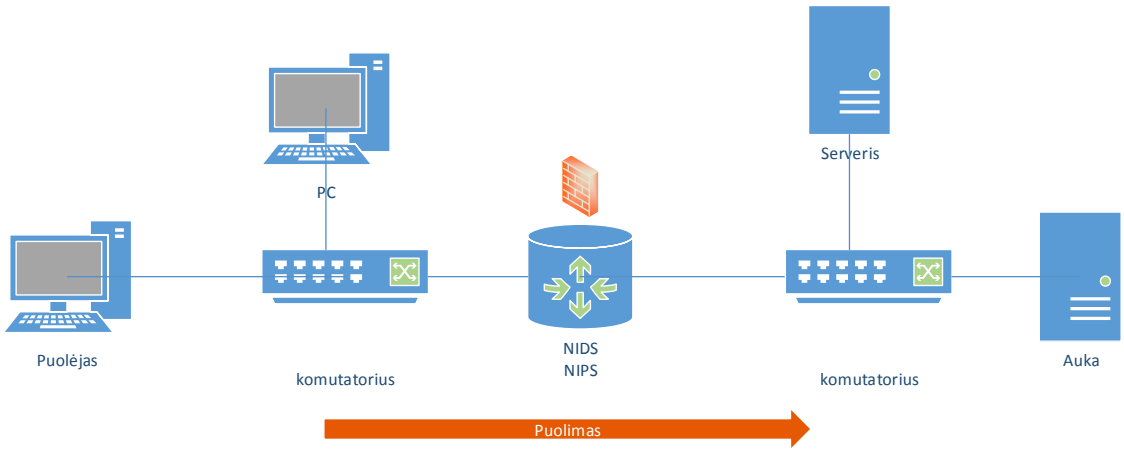
Pasak nacionalinio standartų ir technologijų instituto (angl. *National Institute of Standards and Technology,* NIST) yra keturios įsilaužimų aptikimo sistemų klasės [17]:

- tinklo įsilaužimų aptikimo sistema (angl. *network-based IDS*, NIDS);
- sistemos įsilaužimų aptikimo sistema (angl. *host-based IDS*, HIDS);
- bevielio tinklo įsilaužimų aptikimo sistema;
- tinklo elgsenos analizės sistema (angl. *network behavior analysis systems*, NBA).

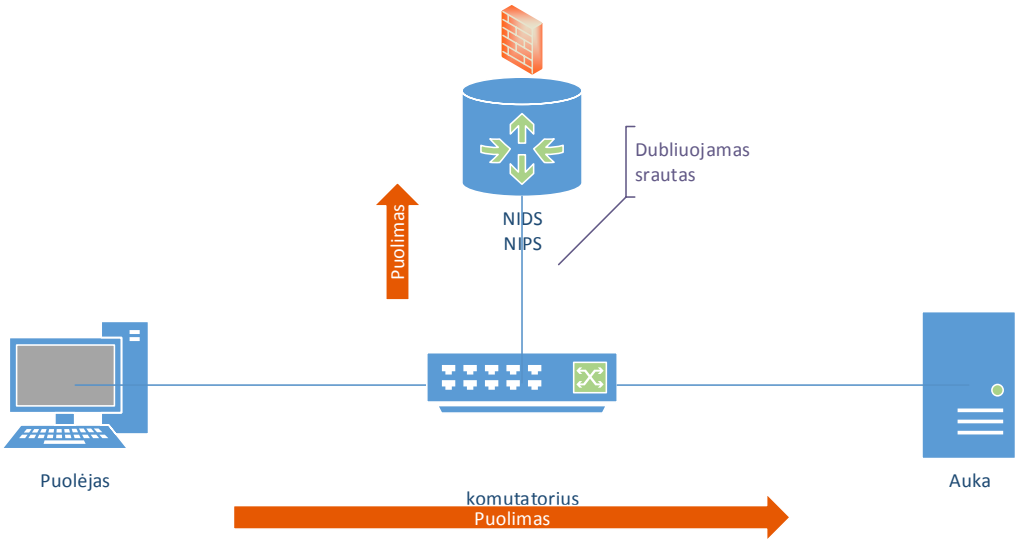
Įsilaužimų prevencijos sistemos (angl. *intrusion prevension system*, IPS) yra skirstomos į tokias pačias klases, kaip ir įsilaužimų aptikimos sistemos – NIPS, HIPS. IPS nuo IDS skiriasi tuo, kad IDS tik generuoja pranešimus, o IPS užblokuoja aptiktą įtartiną srautą.

Tinklo įsilaužimų aptikimo sistema

NIDS/NIPS stebi tinklo srautą, analizuota komunikacijas tarp tinklo įrenginių, transporto ir aplikacijų lygmenyje, kad aptiktų įtartiną veiklą. NIDS gali būti instaliuota į maršrutizavimo įrenginį, kad būtų stebimas visas srautas, einantis tiesiogiai per jį (2.1 pav), arba instaliuotas atskirame įrenginyje ir prijungtas prie „jungiamojo prievado“ (angl. *spanning port*). „Jungiamasis prievadas“ yra specialus komutatoriaus prievadas, kuris visus paketus transmisijos metu nukopijuoja ir išsiunčia į kitą prievadą (2.2 pav.) [17]. Tinklo įsilaužimų aptikimo sistemų pavyzdžiai: Snort IDS, Bro IDS.



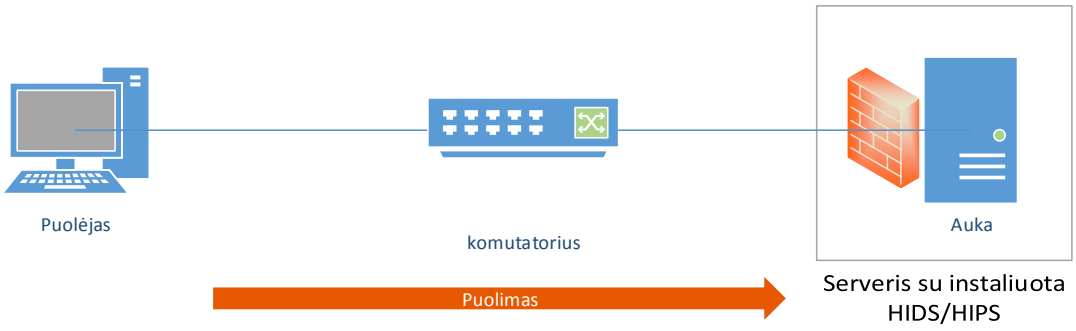
2.1 pav. NIDS/NIPS perimanti srautą



2.2 pav. NIDS/NIPS dubliuojamas srautas

Sistemos įsilaužimų aptikimo sistema

HIDS stebi vienos sistemos veikimo charakteristikas. HIDS į savo algoritmus priima duomenis iš gautų paketų, sisteminių pranešimų, failų integralumo patikros, konfigūracijos patikrinimo, procesų. Kadangi HIDS mato aplikacijų lygmens duomenis, ji gali atpažinti atakas paketuose, kurie yra perduoti saugiu užšifruotu kanalu. Vis dėlto, HIDS negali aptikti daugelio tinklo lygmens atakų, kadangi neturi prieigos prie tinklo lygmens paketų [17]. Sistemos įsilaužimų aptikimo sistemų pavyzdžiai: Tripwire, OSSEC.



2.3 pav. HIDS architektūros pavyzdys

Tinklo elgsenos analizės sistemos

NBA analizuoja tinklo srautą arba tinklo srauto statistiką ieškodama neįprastų komunikacijos atvejų, tokių kaip DDOS atakų, tam tikrų virusų. NBA gali būti įrengtas tinkle identiškai kaip ir NIDS [17].

Bevielio tinklo įsilaužimų aptikimo sistema

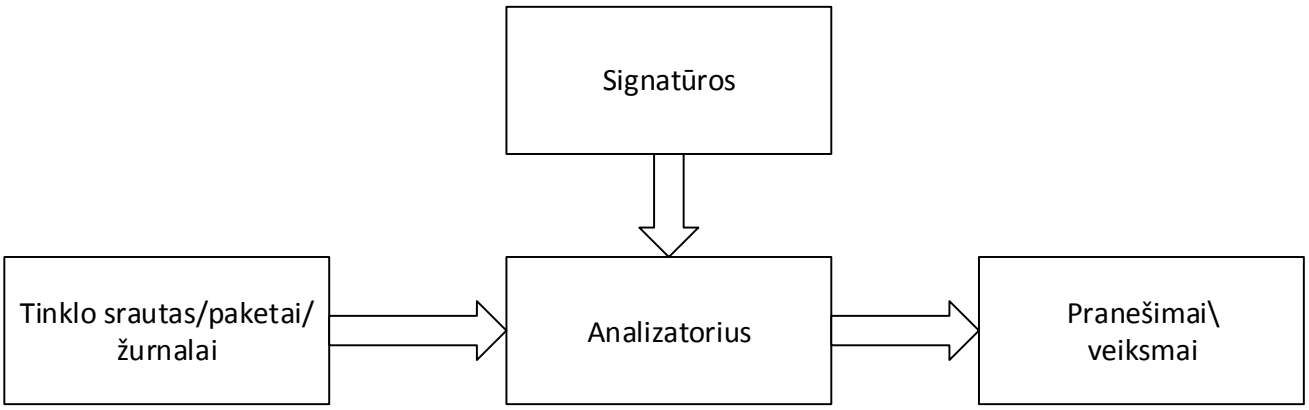
Bevielio tinklo įsilaužimų aptikimo sistema stebi bevielį tinklą ir analizuoja įtartiną veiklą bei naudojamus protokolus [17].

2.2. Signatūrų aptikimas

IDS gali veikti dviem principais:

- Signatūrų aptikimu;
- Anomalijų aptikimu.

Signatūra yra tam tikras modelis ar struktūra, kuri atitinka tam tikrą grėsmę. Signatūromis paremtas įsilaužimų aptikimas yra procesas, kurio metu lyginamos turimos signatūros duomenų bazėje su gautais įvykiais siekiant aptikti potencialius incidentus (2.4 pav.). Įvykis - tai gautas paketas arba paketų kombinacija arba sugeneruoti sisteminiai pranešimai [17].



2.4 pav. Signatūromis paremtos sistemos veikimo modelis

Signatūrų pavyzdžiai:

- Paketas su klaidingomis TCP antraštės vėliavų kombinacijomis;
- Sujungimas tarp dviejų specifinių IP adresų;
- Paketas, siunčiamas į serverio 22 prievadą, turi specifinę eilutę su „root“ savo turinyje.

Signatūromis paremtų įsilaužimų aptikimo sistemų privalumai:

- suprantamumas. Signatūras yra paprasta suprasti, sukurti ir modifikuoti. Kiekviena signatūra tiksliai nurodo sąlygas, kuriomis turi būti sugeneruotas pranešimas arba imtasi atitinkamų veiksmų. Net mažai patirties turintys saugumo administratoriai gali pritaikyti bendras taisykles savo aplinkoje [17];

- tikslumas. Taisyklės yra taip sukurtos, kad būtų kuo mažiau „klaidingai teigiamų“ pranešimų. Kitą vertus, neatsakingai sukurtos taisyklės turės didėlį skaičių „klaidingų pranešimų“. Tokių pranešimų rodiklius yra sunku nuspėti. Jeigu stebimam tinklo sraute vyks aprašyta ataka, ji bus aptikta. Tačiau mes negalime žinoti, kiek atakų signatūrų trūksta [17];

- greitas diegimas. Signatūromis paremtos IDS gali veikti iš karto po jų įdiegimo. Jeigu yra aptikta ataka, daugelis jos požymių yra saugojama, pavyzdžiui, signatūra, šaltinis, gavėjas, laikas. Visas paketo turinys gali būti išsaugomas tolimesnei analizei [17].

Signatūromis paremtų įsilaužimų aptikimo sistemų trūkumai [17]**:**

- neįmanoma aptikti nežinomų atakų, kurių signatūros nėra aprašytos;
- skirtingai atliekamos atakos turi turėti skirtingas, joms pritaikytas signatūras;
- reikia nuolat atnaujinti signatūrų duomenų bazes. Be to, dėl IDS našumo rekomenduojama pašalinti visas signatūras, kurių atakos nėra taikomos konkrečioje aplinkoje.

2.3. Anomalijomis paremtos įsilaužimų aptikimo sistemos

Anomalijų aptikimas tai procesas, kurio metu yra lyginamas standartinės veiklos modelis su realiai stebimais įvykiais aptikti žymius nuokrypius. Tokios IDS naudoja statistiką įsilaužimui aptikti. Jos turi aprašytus arba automatiškai sugeneruotus profilius, kurie apibūdina standartinę veiklą, pavyzdžiui, aplikacijos, vartotojai, komunikacijos, aktyvūs įrenginiai, paketų kiekiai. Tokie profiliai yra sudaromi stebint tinklo ar sistemų veiklą tam tikrą laiko tarpą. Profiliai gali būti statiniai arba dinaminiai. Statiniai profiliai yra pastovūs, o dinaminiai gali adaptuotis atsižvelgiant į pokyčius tinkle [17].

Anomalijų IDS privalumai [17]:

- nežinomų atakų aptikimas. Anomalijų būdu galima aptikti naujas, nežinomas atakas, jeigu jos pakeičia stebimus atributus nuo jų standartinės veiklos;
- vidinių grėsmių aptikimas. Legali veikla, pavyzdžiui, duomenų kopijavimas, gali būti laikoma kaip ataka, jeigu toks veiksmas nebuvo autorizuotas. IDS paremta anomalijų aptikimu gali tokius veiksmus aptikti.

Anomalijų IDS trūkumai [17]:

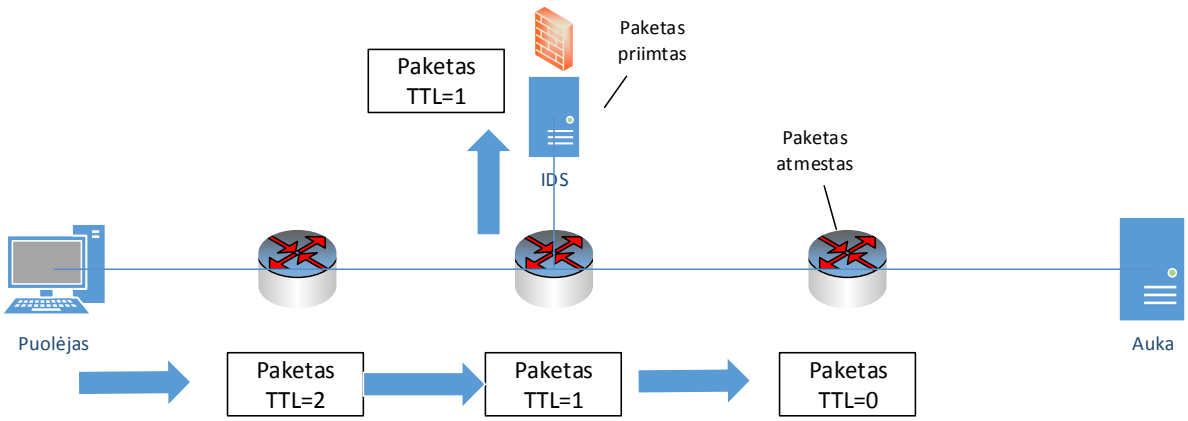
- sudėtingumas. Anomalijų aptikimo sistemos yra sunkiai suprantamos, reikalauja daug investicijų ir žmogiškos veiklos sąnaudų;
- atakų analizės sudėtingumas. Administratorius turi pats surasti pranešimų priežastis. Anomalijų IDS nesuteikia detalios informacijos, tik parodo, kad yra nuokrypis nuo standartinių modelių;
- adaptacijos periodas. Įrengus anomalijų aptikimo sistemą, reikalingas tam tikras laikas, kurio metu generuojami veiklų profiliai. Šiuo periodu IDS negali aptikti atakų.

2.4. Atakos prieš įsilaužimų aptikimo sistemas

Šiuolaikinės IDS yra priklausomos nuo teisingų įvesties duomenų. IDS turi pasiekti identiškus duomenis, kuriuos gauna saugomos sistemos. Įsilaužimų aptikimo sistemos yra pasyvūs įrenginiai, todėl gavus klaidingus duomenis, negali paprašyti jų pakartojimo.

1998 metais [18] buvo aprašytos trys atakų prieš IDS klasės:

- įterpimas. Įterpimo ataka įvyksta tada, kai IDS priima paketą, o aukos serveris jį atmeta. Paketas yra galiojantis tik įsilaužimų aptikimo sistemai. Taip galima apgauti IDS signatūras, įterpiant nereikšmingus paketus. Įterpimo ataką galima pamatyti paveiksle;
- vengimas. Vengimo ataka įvyksta tada, kai IDS atmeta paketą ir aukos serveris jį atmeta;
- DDOS. Tokios atakos tikslas yra išnaudoti visus IDS resursus arba visai išjungti sistemą;
- Šių atakų paskirtis yra desinchronizuoti IDS ir aukos sistemą, kad abu apdorotų skirtingus duomenis.



2.5 pav. Įterpimo atakos pavyzdys

2.4.1. Aptikimo išvengimo būdai

Tinklo lygio aptikimo išvengimo pavyzdžiai [18]:

- TTL atakos. TTL yra atitinkamas laukas paketo antraštėje, kurio reikšmė nusako kiek paketas gali būti maršrutizuojamas, kol turi būti atmestas. Kiekvienas maršrutizatorius TTL reikšmę sumažina vienetu. Puolėjas, žinodamas tinklo architektūrą, gali išsiųsti atitinkamus paketus, kuriuos priims IDS, bet taikinio nepasieks;
- kontrolinės sumos verifikacija. IDS, kuri nepatikrina paketo kontrolinės sumos, yra imli tokiai atakai, nes aukos serveris paketą atmestų;

- šaltinio manipuliacija. Puolėjas gali nurodyti apgaulingą (angl. *spoofed*) šaltinio adresą IP pakete ir kiekvienam savo žingsniui suteikti kitą IP adresą. Tokiu būdu siunčiant paketus, IDS negali tinkamai sekti veiksmus;
- fragmentacija. Tai procesas, kurio metu didelės apimties paketai yra padalinami į mažesnius. Kiekvienas toks fragmentas gauna atskirą IP antraštę ir gali būti maršrutizuojami skirtingais keliais.

Kodo manipuliacijos pavyzdžiai [18]

Per kodo manipuliaciją duomenys gali būti modifikuojami taip, kad IDS jų nesupras. Tokia veikla yra būdinga ir virusams, siekiant išvengti aptikimo. Kodo modifikacijos pavyzdžiai:

- kodavimas (angl. *encoding*);
- šifravimas;
- glaudinimas.

Prievadų skenavimo aptikimo išvengimo pavyzdžiai [18]

Tai atakos laike. Jeigu atvirų prievadų paieška yra paskirstoma dideliame laiko tarpe, IDS negali išlaikyti visos informacijos. V. Bukač [19] atliko įsilaužimų aptikimo sistemos Snort analizę. Jo rezultatus galima pamatyti 2.1 lentelėje. *X* reikšmė lentelėje nurodo laiko intervalą sekundėmis tarp dviejų paketų. Snort įrankis turi prievadų skenavimo aptikimo modulį „sfPortscan“ su skirtingais jautrumo lygiais: mažas, vidutinis, aukštas.

2.1 lentelė Snort programos aptikimo išvengimo tyrimo rezultatai **[19]**

sfPortscan	Žemas		Vidutinis		Aukštas	
Ugniasienė	Įjungta	Išjungta	Įjungta	Išjungta	Įjungta	Išjungta
X=76	Neaptikta	Neaptikta	Neaptikta	Neaptikta	Neaptikta	Neaptikta
X=65	Neaptikta	Neaptikta	Neaptikta	Neaptikta	Neaptikta	Aptikta
X=16	Neaptikta	Neaptikta	Neaptikta	Neaptikta	Neaptikta	Aptikta
X=15	Neaptikta	Aptikta	Neaptikta	Neaptikta	Neaptikta	Aptikta
X=6.5	Neaptikta	Aptikta	Neaptikta	Neaptikta	Neaptikta	Aptikta
X=6.3	Neaptikta	Aptikta	Neaptikta	Aptikta	Neaptikta	Aptikta
X=3.1	Neaptikta	Aptikta	Neaptikta	Aptikta	Neaptikta	Aptikta
X=3.0	Neaptikta	Aptikta	Neaptikta	Aptikta	Neaptikta	Aptikta
X=0.65	Neaptikta	Aptikta	Neaptikta	Aptikta	Aptikta	Aptikta
X=0.47	Neaptikta	Aptikta	Neaptikta	Aptikta	Aptikta	Aptikta
X=0.44	Neaptikta	Aptikta	Aptikta	Aptikta	Aptikta	Aptikta

X=.033	Neaptikta	Aptikta	Aptikta	Aptikta	Aptikta	Aptikta

Rezultate matosi, kad dideliais laiko intervalais skenuojant sistemą galima išvengti aptikimo. Taip pat galime pastebėti, kad lengviau yra išvengti aptikimo, jeigu įrenginys yra apsaugotas ugniasiene. Taip nutinka, nes uždarytas prievadas siunčia RST pranešimą atgal, o ugniasienė jokio atsakymo neduoda filtruodama prievadus. RST pranešimai yra naudojami prievadų skenavimo aptikimo algoritmuose.

Z. Jammes [20] atliko Snort sistemos tyrimą prieš NMAP įrankio tinklo skenavimą (rezultatai lentelėje). Pirmojo stulpelio reikšmės yra NMAP intervalų parametras „T [0 – 5]“ kur 5 reiškia greičiausią skenavimą, o 0 – lėčiausią, 15 min. laiko intervalą tarp paketų. Rezultatai buvo panašūs. Skenuojant dideliais intervalais įsilaužimų aptikimo sistema nepranešė apie prievadų skenavimą.

2.2 lentelė NMAP skenavimo rezultatai prieš Snort **[20]**

SYN skenavimas	Aptikimas
T5	Aptiko
T4	Aptiko
T3	Aptiko
T2	Aptiko
T1	Aptiko
T0	Neaptiko

2.5. Pramoninių tinklų įsilaužimų aptikimo sistemos

Kaip taisyklė, pramoniniuose tinkluose nėra naudojamos HIDS/HIPS tipo sistemos, kadangi ne visi ICS komponentai palaiko šias sistemas. NIDS yra dažniausiai naudojamos technologiniuose tinkluose, kadangi NIPS blokavimo galimybės sukelia per didelę riziką kritinėms sistemoms, kurios priklauso nuo visų modulių pasiekiamumo. Belieka rinktis iš dviejų metodų: anomalijų aptikimo ir signatūrų aptikimo. Signatūroms paremta IDS turi savo privalumų, tačiau pažeidžiamumas yra žinomas tada, kada jis yra išnaudotas. Kompanija „Digital Bond“ yra išleidusi rinkinį taisyklių, skirtų Modbus protokolui [21]. Šios taisyklės aprašo Modbus protokolo naudojimą, protokolo klaidas ir tinklo skenavimą . Tradicinėmis signatūromis paremtos IDS galėtų aptikti primityvias atakas. Tačiau kaip aprašyta [22], SCADA atakos gali būti ypatingai kompleksiškos, retai įgyvendinamos vienu ar keliais žingsniais, pavyzdžiui, vienos saugumo spragos išnaudojimas. Dėl to yra svarbu gebėti aptikti kompleksiškas ir pavojingas atakas.

Daugelis mokslinių tyrimų darbų teigia, kad anomalijų aptikimo metodas yra pranašesnis už taisyklėmis pagrįstų įsilaužimo aptikimo metodą. Technologiniai tinklai yra labiau nuspėjami,

lyginant su IT. Jie veikia reguliariais ir žinomais modeliais, ir nuolat atlieka tuos pačius veiksmus. Įvairūs anomalijų aptikimų metodai yra analizuojami sekančiame skyriuje.

2.5.1. Išanalizuoti modeliai

Düssel P. [23] pasiūlė paketų turinio (angl. *payload*) paremtą realaus laiko anomalijų sistemą. Jų sistema nepriklauso nuo protokolo ir gali aptikti nežinomas atakas. Šis metodas remiasi pramonių tinklų pastovumo charakteristika. Yra siūlomi keturi sistemos komponentai: tinklo sensorius, ypatybių klasifikavimo modulis, panašumų aptikimo modulis, anomalijų modulis. Tinklo sensorius surenka paketus, pasinaudodamas Bro IDS. Tuomet paketų turinys išimamas ir nusiunčiamas į ypatybių klasifikatorių. Paketo bitų sekos yra išdėliojamos matricoje. Kitas komponentas atranda ir užregistruoja sekų panašumus. Galiausiai, anomalijų aptikimo modulis sulygina esamą tinklo srautą su normalia elgsena ir nesutapimai yra traktuojami kaip anomalijos.

Cheung S. [24] pasiūlė trijų lygių modelių principu paremtą sistemą Modbus TCP komunikacijų stebėjimui. Jis siūlo sukonstruoti ir apsirašyti modelius, kurie charakterizuoja tipinį sistemų veikimą ir aptinka nukrypimus kaip anomalijas. Yra siūlomi trijų tipų modeliai: protokolų lygio, komunikacijų lygio ir pasiekiamumo. Protokolų lygio modeliai buvo pasirinkti charakterizuoti Modbus TCP užklausas ir atsakymus pagal protokolo specifikacijos dokumentacijas.

Valdes A. [25] pademonstravo, kaip galima panaudoti anomalijų aptikimų metodus, paremtus adaptacija arba prisitaikytinu mokymusi (angl. *adaptive learning*), aptinkant įsilaužimus pramonės valdymo tinkluose. Jie aprašė du metodus: struktūromis paremtą anomalijų aptikimą ir srautais paremtą anomalijų aptikimą. Abu metodai savo matematinėse formulėse formuoja standartines sistemų veikimo charakteristikas iš šaltinio IP ir galutinio IP adresų naudojamų prievadų. Rezultatuose paaiškėjo, kad srautais paremtų anomalijų aptikimo metodas geriau aptiko nuokrypius lyginant su standartinių komunikacijų modeliu.

Igor Nai F. [26] pabrėžė, kad atakos prieš ICS ne visada gali būti aptiktos tinklo sraute kaip anomalijos. Jo komanda pasiūlė metodą, paremtą konkrečių įrenginių kritine stadija. Pavyzdžiui, sistema sudeda iš vandens pompų su dviem vožtuvais. Abu vožtuvai yra kontroliuojami iš SCADA serverio, tačiau tik vienas tūrėtų būti uždarytas bet kuriuo metu. Jeigu yra uždaromi abu vožtuvai, gali atsirasti grėsmė sistemos veiklai, todėl atsiranda kritinė situacija. Tokiu principu paremtas metodas siekia aptikti atakas, kaip įsilaužėlis turi visą SCADA sistemos kontrolę ir pakenkti sunkiai aptinkamais veiksmais.

2.5.2. Anomalijų aptikimo sistemų trūkumai

Išanalizavus siūlomus metodus keli dalykai yra akivaizdūs. Pirmiausia, visi metodai buvo realizuoti bandomojoje aplinkoje, kur srautai ir įrenginiai buvo simuliuoti. Nei vienas metodas nebuvo išbandytas realioje aplinkoje, kur įrenginių ir srautų kiekiai yra dideli. Po to, visi tyrėjai savo

išvadose teigė, kad jų metodai generavo nemažai klaidingų pranešimų. Tokių sprendimų pritaikymas realiame tinkle pareikalautų daug papildomų investicijų ir žmogiškųjų išteklių.

Kita esminė problema su anomalijų sistemomis - jos stebi pačių pramoninių sistemų tarpusavio veiklas, o ne žmonių sąveiką su sistemomis. Sistemų tarpusavio veiksmai ir komunikacijos yra nuspėjamos, pastovios, o žmonių veiksmai ne. Identifikuotos trys vietos, kuriose anomalijų aptikimo sistemos gali būti neveiksmingos: VPN prieigos vieta, SCADA valdymo vietos ir nutolusių sistemų valdymo vietos, pavyzdžiui, elektros tinklo pastotės. Metodai, kurie siūlo aprašyti veikimo charakteristikas, susidurs su problema, kad tinkamai aprašyti žmonių sąveiką su sistemomis yra sudėtinga. Galima charakterizuoti naudojamus prievadus, servisus, aplikacijas, bet reikia atsižlėgti į tai, kad pramonės tinklus gali sudaryti keli šimtai įrenginių. Be to, yra rizika, kad įsilaužėliai puls per tuos pačius naudojamus protokolus ir prievadus, prisidengę inžinierių paskyromis, kaip buvo Ukrainos atveju. Turinio tokios sistemos netikrina, todėl jame gali slėptis, pavyzdžiui, kenksminga sistemos atnaujinimo programinė įranga.

Metodai, kurie siūlo automatiškai prisitaikyti prie elgsenos charakteristikų, susidurs su panašia problema - kaip stebėjimo ir adaptacijos laikotarpiu įvertinti visus žmonių galimus veiksmus su sistemomis. Inžinierius gali jungtis į vieną įrenginį tik tuo metu, kai iškyla problemos, o jos gali atsirasti nuolat, arba beveik niekada. Taip pat, gali keistis trečiųjų šalių palaikymas, jų naudojami įrankiai ar protokolai. Adaptacijos periodas yra ribotas ir per jį neįmanoma apžvelgti visų žmonių sąveikos su sistemomis veiksmų. Kiekvienas naujas įvykis generuos pranešinus priklausimai nuo metodo jautrumo ir kiekvienam tyrimui reikės resursų. Jeigu sprendimas generuoja įspėjimus esant tik dideliems nuokrypiams, iškyla rizika, kad minimali, neakivaizdi piktybinė veikla liks nepastebėta bendrame sraute.

2.6. Išvados

Jeigu grįžti prie įsilaužimo veiksmų vidiniame tinkle, yra trys pagrindiniai etapai: žvalgyba, išplitimas/atakos, žalos sukėlimas. Signatūromis paremtos IDS yra skirtos aptikti pirmus du atakos etapus, tačiau žvalgyba gali būti paslepiama, o dėl mažo kiekio žinomų ICS pažeidžiamumų, išplitimo ar atakos viduje signatūra gali būti neaptikta. Visi išanalizuoti anomalijų įsilaužimų aptikimo metodai labiausiai pritaikyti aptikti sistemų veikimo nuokrypius, t.y. trečiąjį įsilaužimo etapą, kai sistemos jau paveiktos ir funkcionuoja ne pagal paskirtį. Priklausomai nuo metodo, galima pastebėti ir ankstesnių žingsnių veiksmus, tačiau tai priklauso nuo sistemos jautrumo ir naudojamo metodo.

Vis dėlto, negalima paneigti siūlomų metodų veikimo principų, tačiau akivaizdu, kad stebėti ir analizuoti kiekvieną pranešimą, kurių bus daug, pareikalaus daug išteklių ir nuolatinės priežiūros.

3. ĮSILAUŽIMŲ APTIKIMO SISTEMOS KONCEPCIJA IR MODELIS

3.1. Sprendžiama problema

Kadangi ICS yra priskirtos prie kritinės infrastruktūros ir labiau pažeidžiamos negu standartinės IT sistemos, reikia kuo greičiau aptikti įsilaužimą technologiniame tinkle. Pirmas veiksmas patekus į vidinį tinklą yra žvalgyba. 2.5 skyriuje buvo identifikuotos vietos, kuriose anomalijų aptikimo sistemos gali būti neveiksmingos: VPN prieigos vieta, SCADA valdymo vietos ir nutolusių sistemų valdymo vietos. Šiose vietose būtina sustiprinti saugumą. 2.4 skyriuje buvo aptarta problema dėl įsilaužimų aptikimo sistemų išvengimo tinklo skenavimo metu. Šis pažeidžiamumas atsiranda dėl to, kad IDS algoritmai negali aptikti tinklo žvalgybos veiksmų, jeigu jie imituoja standartinius administratoriaus veiksmus ir yra specialūs būdai aptikimo išvengimui.

IDS taip pat neaptinka viruso plitimo tinkle, jeigu nėra žinoma jo signatūra. Virusai tinkle ieško aktyvių įrenginių, kreipdamiesi į visus IP adresus. Tai dažniausiai būna konkretus prievadas, nes įsilaužtdamas į sistemą virusas išnaudoja konkretaus serviso saugumo spragą [27]. Šioms rizikoms sumažinti yra siūloma sistema, kuri aptiktų tinklo žvalgybos veiksmus.

3.2. Kuriamos sistemos modelis

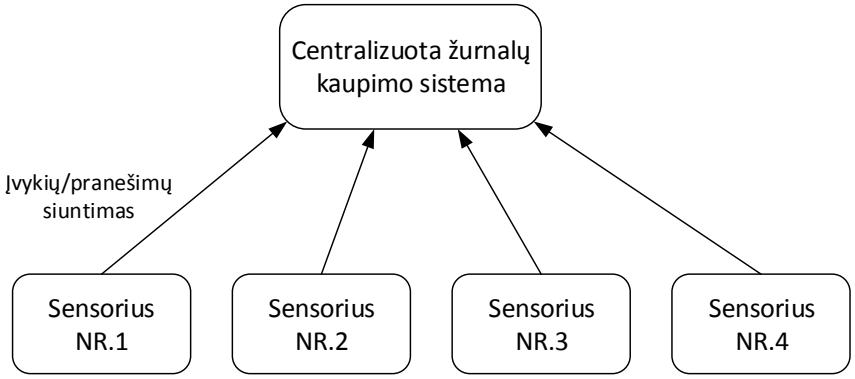
Įsilaužėlis į vidinį tinklą pirmiausiai patenka per vieną įrenginį. Tai gali būti pažeistas kompiuteris arba sistema su atgalinėmis durimis, nuotolinės prieigos taškas. Taip pat į tinklą galima patekti per nesaugų bevielį ryšį arba fiziškai prisijungus prie tinklo. Tačiau dažniausiai įsilaužėlis neturi aukos tinklo architektūros. Norėdamas tęsti kenkėjiškus veiksmus, turi surasti ir identifikuoti veikiančias sistemas, saugos įrenginius, darbo vietas, potinklius, DMZ.

Atsižvengiant į tai, yra siūloma sukurti sistemą, kuri aptiktų aktyvių IP adresų paiešką tinkle.

Sistema priimtų tokius paketus:

- ICMP
- TCP
- UDP

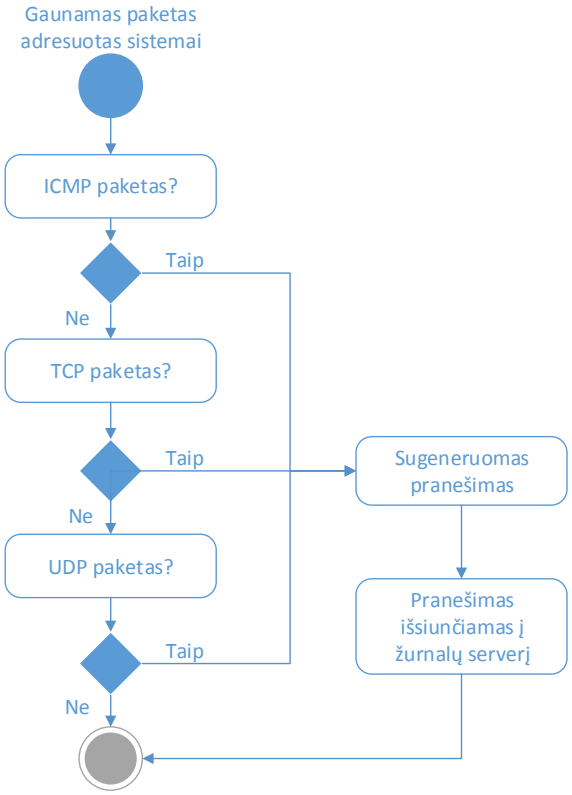
Po gauto paketo (3.2 pav.) sistema sugeneruotų ir išsiųstų pranešimą į centralizuotą žurnalų kaupimo serverį. Sistemos veikimą galima pamatyti 3.1 pav.



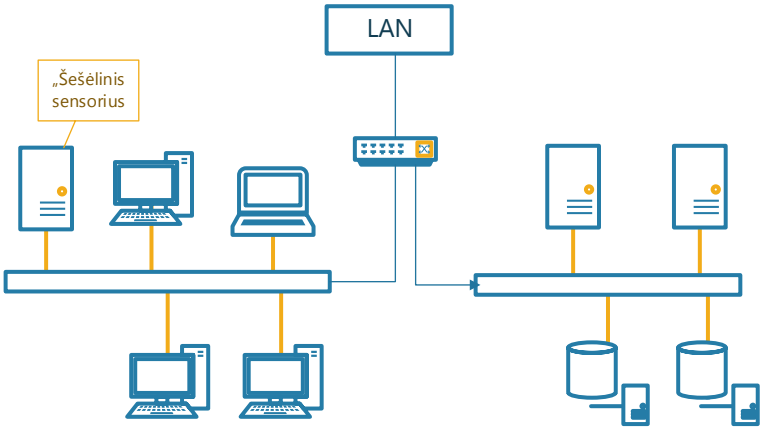
3.1 pav. Siūlomos sistemos architektūra

3.2.1. Sistemos veikimo pagrindimas

Tai būtų kaip sensorius, pastatytas strategiškai svarbiose vietose ir reaguojantis į visus komunikacijų srautus, ateinančius į jį. Jeigu technologiniame tinkle yra sistemos ir įrenginiai, kurie nuolatos komunikuoja tarpusavyje, į juos jungiasi administratoriai, trečiosios šalys ar gamintojai, tai šis sprendimas patalpintų „šešėlinę“ sistemą šalia tikrųjų. Tai parodyta 3.3 pav.

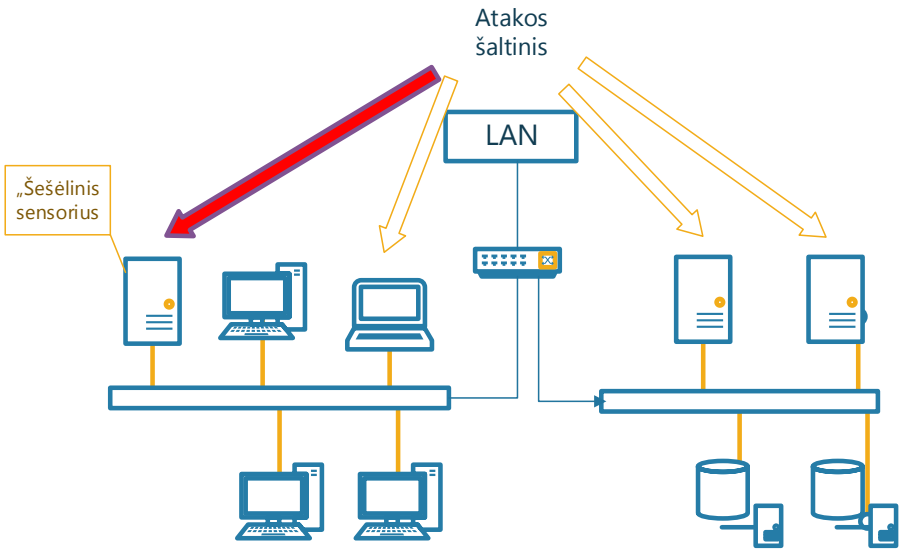


3.2 pav. Sistemos algoritmo veikimas



3.3 pav. Sensoriaus vieta tinkle

Apie jos egzistavimą turi žinoti kuo mažiau žmonių, nes teoriškai tokios sistemos niekas neprižiūri, niekas nesinaudoja ir niekas neturėtų generuoti duomenų srautus į ją. Jeigu bandyti apsaugoti realią sistemą arba įrenginį nuo, pavyzdžiui, prievadų skenavimo, galima susidurti su problema, kai tai gali atlikti ir administratoriai, gamintojai, tikrindami įrenginio veikimą arba saugumo skyriaus darbuotojai, tikrindami sistemą. Įsilaužimo arba viruso plitimo atveju, yra ieškoma įrenginių ir sistemų potencialiai atakai ir tai galima padaryti, pavyzdžiui, siunčiant ICMP ECHO pranešinus kiekvienam IP adresui (2.4 pav.). IPS sistemos to gali ir neaptikti, jeigu tokia veikla būdinga ir tų sistemų administratoriams, skenavimas atliekamas retais laiko intervalais arba aktyviai naudojamos priemonės aptikimo išvengimui. Būtent šiuo atveju „šešėlinė“ sistema įgytų pranašumą prieš standartines IPS sistemas, nes jos principas yra reaguoti ir pranešti apie visas komunikacijas, visus ECHO paketus ir prisijungimus. Tai būtu netikra sistema, ja niekas neturėtų naudotis, todėl komunikacija į ją yra tikėtinas neteisėtos veiklos požymis.



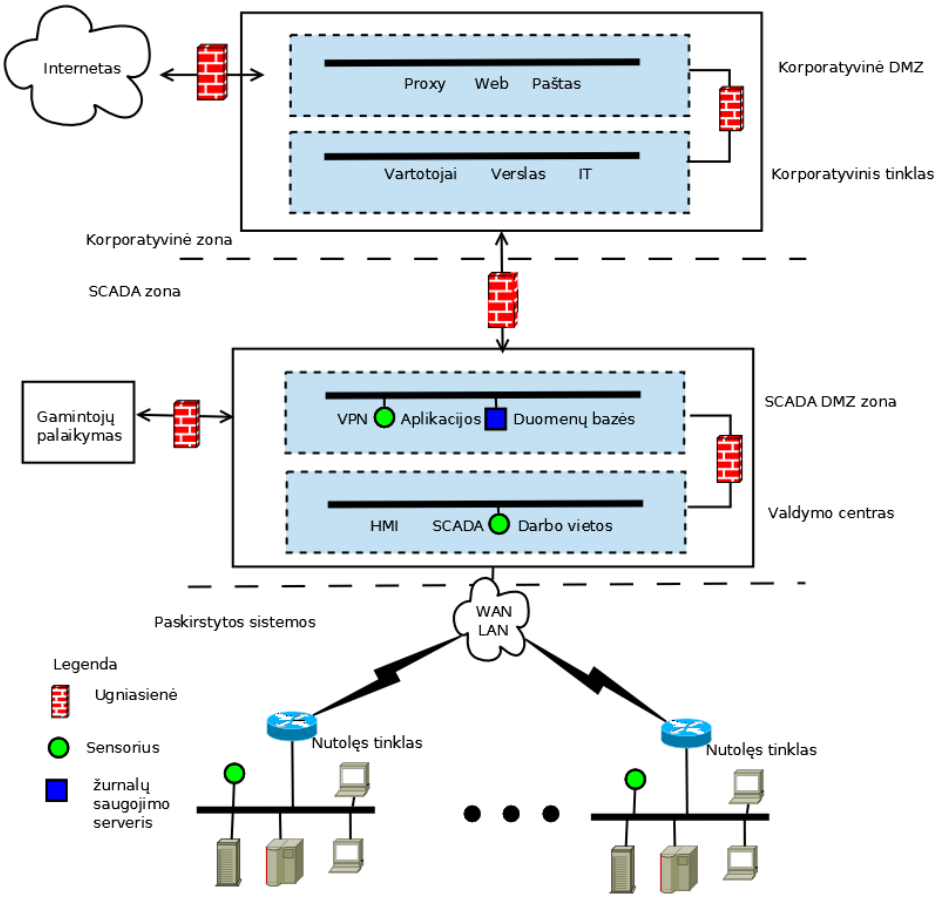
3.4 pav. Tinklo žvalgyba

3.2.2. Sensoriaus architektūra pramoniniame tinkle

Norint nuspręsti, kurioje tinklo dalyje sensoriai turėtų būti įrengti, pirmiausia reikia identifikuoti vietas, kuriose yra didžiausia rizika, kad įsilaužėlis pateks į SCADA tinklą. Siūloma pirmiausia įrengti sistemą šiuose vietose:

- demilitarizuota SCADA zona, nes šioje vietoje susijungia technologiniai ir korporatyviniai tinklai. Tokiose vietose yra sistemos, kurios yra pasiekiamos iš abiejų tinklų;
- VPN prieigos terminavimo vietos. Dažniausiai VPN prieiga terminuojama ant vidinių ugniasienių ir taip suteikia prieigą autorizuotiems vartotojams į atitinkamas technologinio tinklo dalis. Ukrainos incidento atveju į SCADA tinklą įsilaužėliai pateko būtent per VPN prieigą ir toliau imitavo tikro inžinieriaus veiksmus. Dėl to, siūloma sensorius turėti visuose potinkliuose, į kuriuos prieiga yra suteikiama per VPN;
- SCADA sistemos potinklyje;
- nutolusiuose tinkluose, pavyzdžiui, pastotėse.

Centralizuotas žurnalų saugojimo serveris turėtų būti DMZ zonoje. Siūlomas sensorių vietas tinkle galima pamatyti 3.5 pav.



3.5 pav. Siūlomo sprendimo vietos tinkle

3.3. Sistemos saugumas

Diegiant sensorių yra privaloma jo konfigūraciją „užgrūdinti“ jį (angl. *hardening*), atsižvelgiant į saugumo rekomendacijas pramonės tinklams (1.8 skyrius). Saugumo konfigūraciją galima išskirstyti į tris dalis:

- sensoriaus saugumas;
- žurnalų saugojimo serverio saugumas;
- komunikacijos tarp jų patikimumas.

Sensoriaus saugumas

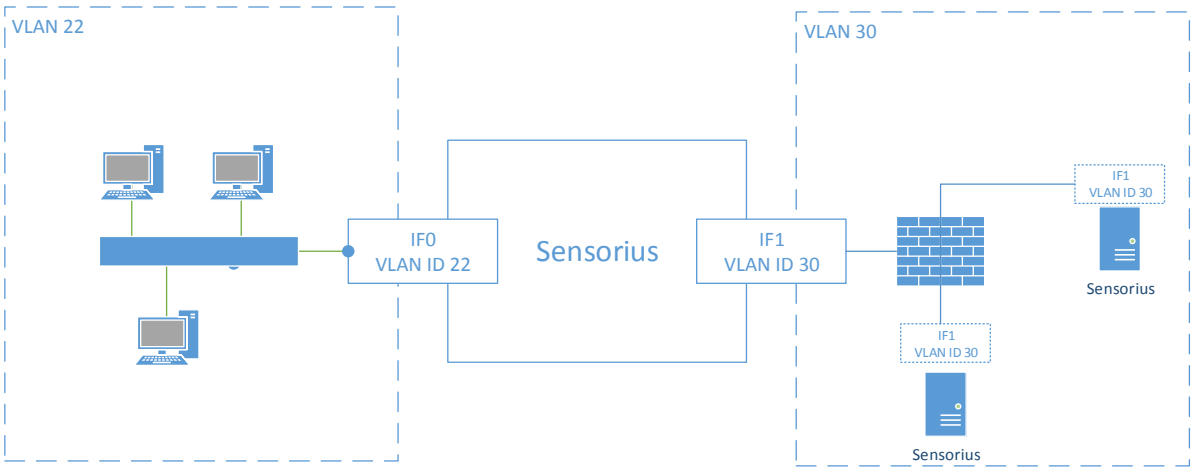
Sensoriuje turi būti dvi tinklo sąsajos (IF0 ir IF1) su skirtingais IP adresais. Suteikti adresai privalo būti skirtinguose virtualiuose vietiniuose tinkluose (angl. *virtual private network* - VLAN):

- IF0 turi priklausyti virtualiam vietiniam tinklui, kuriame yra saugojami įrenginiai;
- IF1 turi priklausyti atskirai dedikuotam virtualiam vietiniam tinklui sensorių konfigūracijai.

Sensoriaus ugniasienės konfigūracija:

- IF0 ugniasienės konfigūracija turi drausti bet kokį įeinantį ir išeinantį tinklo srautą;
- IF1 ugniasienės konfigūracija turi praleisti įeinančias SSH sesijas prie 22 prievado.

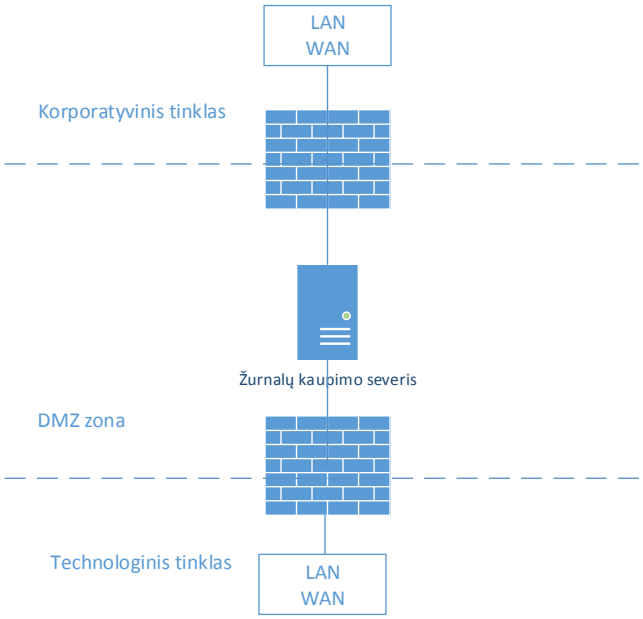
IF0 sąsają reikia uždaryti, kad esant įsilaužimui tinkle sensorius nebūtų potencialus taikinys. O tuo atveju, jeigu pats įrenginys bus kompromituotas, jis negalės pulti kitų tame pačiame potinklyje esančių sistemų. Įeinančio srauto uždarymas per ugniasienę nesutrikdys sistemos darbo, nes paketai yra pagaunami prieš juos apdorojant ugniasienei (3.4 skyrius). IF1 turi priimti tik SSH srauto protokolą nuotolinio administravimo darbams atlikti.



3.6 pav. Sprendimo tinklo sąsajos

Žurnalų saugojimo serverio saugumas

Žurnalų serveris turi būti įrengtas technologinio tinklo DMZ zonoje, tame pačiame virtualiame vietiniame tinkle, kaip ir sensoriai. Kadangi žurnalų serveris būtų patalpintas tarpinėje zonoje tarp korporatyvinio ir technologinio tinklo (3.7 pav), prieigos apribojimą yra nesudėtinga realizuoti.



3.7 pav. Žurnalų saugojimo serverio vieta tinkle

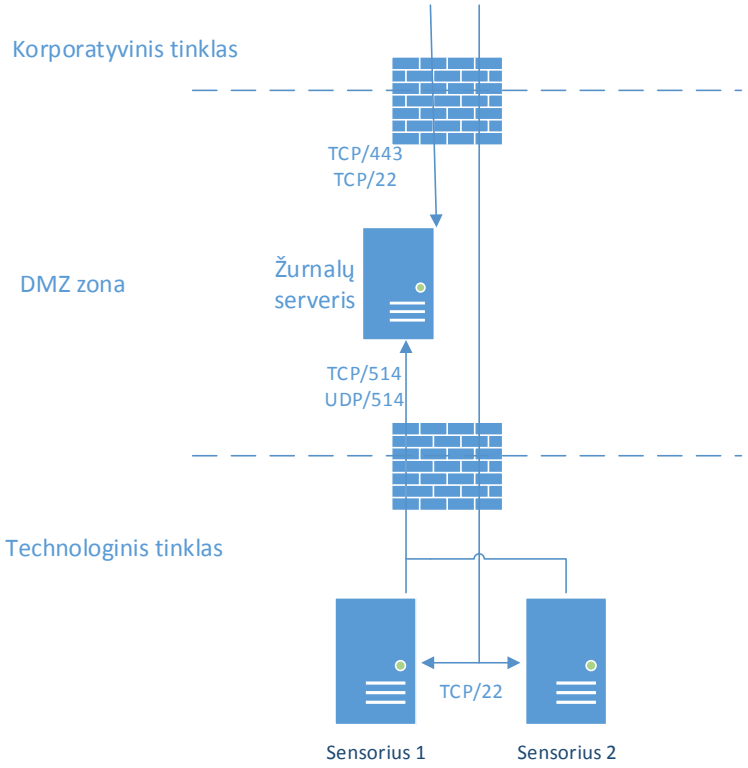
Žurnalų serveriui rekomenduojama atidaryti šiuos prievadus:

- TCP/22 administravimui;
- TCP/443 standartiniam prisijungimui prie sistemos;
- TCP/514, UDP/514 standartiniai sisteminių žurnalų (angl. „Syslog“) priėmimo prievadai.

Prievadai gali būti ir kitokie, jeigu papildomam saugumui užtikrini atitinkami servisai yra sukonfigūruoti ant nestandartinių prievadų. Tiek standartiniam darbui, tiek administravimui tiesiogiai iš korporatyvinio tinklo, pasiekti sistemą nerekomenduojama. Siūloma identifikuoti asmenis, kuriems bus reikalinga prieiga prie sistemos ir prieigą suteikti per vidinės ugniasienės VPN. Tokiu būdu bus užtikrinta, kad esant įsilaužimui korporatyviniame tinkle, sistema nebus pasiekiama tiesiogiai.

Komunikacijų srautai

Sensoriai vienas kito pasiekti tinkle neturėtų. Kaip parodyta 3.8 pav. sensoriai priima tik saugias komunikacijas 22 prievadu, o žurnalų serveris iš technologinės pusės priima sisteminius žurnalus per 514 prievadą, o iš korporatyvinės VPN terminavimosi dalies – 22 ir 443 prievadus. Esant poreikiui, atidaromas SMTP prievadas, norint siųsti pranešimus paštu suinteresuotiems asmenims.



3.8 pav. Siūlomo sprendimo komunikacijos srautai

Pastabos ir rekomendacijos:

- Sistemos IP adresų ir vietų tinkle dokumentuoti nerekomeduojama, kadangi nutekėjus informacijai apie tinklo infrastuktūrą, būtų sužinota apie sistemos egzistavimą;
- Ieškant aktyvių įrenginių dar galima užklausiant ir vidinį DNS serverį. Todėl siūloma kiekvienam sensoriui sutekti vardą DNS serveryje, tačiau akivaizdžiai nenurodyti jo paskirties, pavyzdžiui, „*AGA001.domenas.lt*“.

3.4. Prototipo realizacija

Vienas iš būdų, kaip paprastai ir efektyviai realizuoti sistemos koncepciją, yra panaudoti jau esamas įsilaužimų aptikimo sistemas. Kadangi jos priima ir analizuoja bet kokį tinklo srautą, ateinantį į fizinę sąsają, modifikavus taisykles galima gauti norimą siūlomos sistemos prototipą. Šiuo atveju buvo pasirinkta Snort įsilaužimų aptikimo sistema. Sistemos diegimo ir konfigūravimo eigos seka:

1. Pasirenkama Snort palaikanti operacijų sistema;
2. Į ją įdiegiama Snort įsilaužimų aptikimo sistema;
3. Atliekama konfigūracija, kuri suteiks Snort įrankiui aprašytos sistemos funkcionalumą;
4. Įdiegiama žurnalų kaupimo ir saugojimo sistema;
5. Atliekama abiejų sistemų saugumo konfigūracija.

Kad Snort įrankis įgytų sensoriaus funkcionalumą, reikia atlikti tam tikrus konfigūracinius veiksmus. Pirmiausia, į dokumentą pavadinimu “local.rules” (numatytoji vieta Linux sistemoje – „/etc/snort/rules/local.rules”) suvesti tokias taisykles:

1. *alert icmp any any -> $HOME_NET any (msg:"Aptiktas ICMP paketas"; sid:10000001; classtype:attempted-recon;);*
2. *alert tcp any any -> $HOME_NET any (msg:"Aptiktas TCP paketas"; sid:10000002; classtype:attempted-recon;);*
3. *alert udp any any -> $HOME_NET any (msg:"Aptiktas UDP paketas"; sid:10000003; classtype:attempted-recon;);*

Taisyklių reikšmių ir parametrų paaiškinimai

Standartinis Snort taisyklių šablonas atrodo taip:

veiksmas protokolas šaltinio_IP šaltinio_prievadas kryptis gavėvo_IP gavėjo_prievadas (parametrai)

Atitinkamai parašytos taisyklės:

- „veiksmas“ – sugeneruojamas pranešimas „alert“;
- „protokolas“ – ICMP, TCP ir UDP;
- „šaltinio_IP“ – pranešimai, generuojami esant bet kokiam šaltiniui „any“;
- „šaltinio_prievadas“ - pranešimai generuojami esant bet kokiam šaltinio prievadui „any“;
- „kryptis“ – įeinantys paketai „->“;
- „gavėvo_IP“ – įrenginiui suteiktas IP adresas, kuris priskirtas kintamajam - „$HOME_NET“;
- „gavėjo_prievadas“ – bet koks gavėjo prievadas „any“;
- „parametrai“ – papildomi kintamieji, suteikiantys reikšmę pranešimui. Šiuo atveju:
    - „msg:“ – taisyklės aprašas;
    - „sid:“ – unikalus taisyklės identifikatorius;
    - „classtype:“ – taisyklės klasė, kuri yra suprantama kitoms programoms apdorojant pranešimą.

Po taisyklių seka pagrindinio nustatymų dokumento „snort.conf“ (numatytoji vieta Linux sistemoje – „/etc/snort/ snort.conf”) konfigūracija. Dokumente reikia nurodyti „$HOME_NET“ kintamojo reikšmę į sistemai suteikto IP adreso reikšmę ir užkomentuoti visas kitas taisykles. Pasirinkti žurnalų kaupimo ir saugojimo sistemą galima iš jau esamų komercinių arba nemokamų sprendimų. Remontuojama naudoti „Graylog“ atviro kodo sisteminių žurnalų rinkimo sistemą.

Sensorius aktyvuojamas tokia komanda:

sudo /usr/local/bin/snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i eth0

Komandos paaiškinimai:

- -A console – pranešimai generuojami į tą pačią konsolę;
- -q – tylusis rėžimas;
- -u snort – nurodomas vartotojas;
- -g snort – nurodoma vartotojo grupė;
- -c /etc/snort/snort.conf – nurodomas kelias iki pagrindinio konfigūracijos dokumento;

- -i eth0 – tinklo sąsaja, kurią reikia stebėti.

3.5. Apibendrinimas

Siūlomo sprendimo privalumai:

- sąlyginai greitas konfigūravimas ir diegimas;
- nėra įtakos kitoms sistemoms.

Trūkumai:

- netiesiogiai saugo tinklą;
- sužinojus apie tokios sistemos egzistavimą, galima ją apeiti.

Šis sprendimas yra greitai realizuojamas, neturi įtakos kitoms sistemos, negeneruoja daug duomenų srautų. Turint tokią sistemą strategiškuose tinklo vietose, padidėja tikimybė aptikti įsilaužimą prieš piktavaliui puolant kitas sistemas. Tokiu pačiu principu galima aptikti ir dar nežinomus virusus, kurie plisdami po tinklą, ieško aktyvių sistemų. Tačiau įsilaužimo aptikimas nėra garantuotas, kadangi šis sprendimas sistemas saugo netiesiogiai. Atsitiktinai praleidus šio įrenginio skenavimą, mano siūlomas sprendimas bandymo įsilaužti į sistemą neaptiks.

4. TINKLO ŽVALGYBOS APTIKIMO TYRIMAS

4.1. Tyrimo tikslas

Šiuo tyrimu buvo siekta parodyti kaip įsilaužimų aptikimo sistemos aptinka tinklo žvalgybos ir sistemų skenavimo veiksmus, bei pademonstruoti, kaip veikia siūlomos sistemos prototipas.

4.2. Tyrimo aplinka

Įrenginiai ir sistemos

Ištirti įsilaužimų aptikimo sistemos veikimą buvo paruošta bandomoji aplinka, kurią sudarė tokie įrenginiai:

- PC1 – kompiuteris su Windows 8 operacine sistema;
- PC2 – kompiuteris su Windows 7 operacine sistema;
- PC3 – kompiuteris su Linux operacine sistema;
- DEV1 – SCADA sistemos „Medaus puodynės“ tipo virtualus įrenginys Siemens S7-200 CPU [28].

IDS

Tyrimui buvo pasirinkta ir sukonfigūruota Snort įsilaužimų aptikimo sistema su tokiais parametrais:

- saugomas potinklis: 192.168.0.0 /24;
- įjungtas „sfPortscan“ tinklo skenavimo aptikimo modulis;
- įjungtos „Scan“ tipo taisyklės iš viešai prieinamų nemokamų taisyklių.

```
422 Snort rules read
    4 detection rules
    150 decoder rules
    268 preprocessor rules
422 Option Chains linked into 2 Chain Headers
0 Dynamic rules
+++++++++++++++++++++++++++++++++++++++++++++++++++

+-------------------[Rule Port Counts]---------------------------------------
|             tcp     udp    icmp      ip
|     src       0       0       0       0
|     dst       4       0       0       0
|     any     418       0       0       0
|      nc     422       0       0       0
|     s+d       0       0       0       0
+------------------------------------------------------------------------------
```

4.1 pav. Aktyvuotos Snort taisyklės

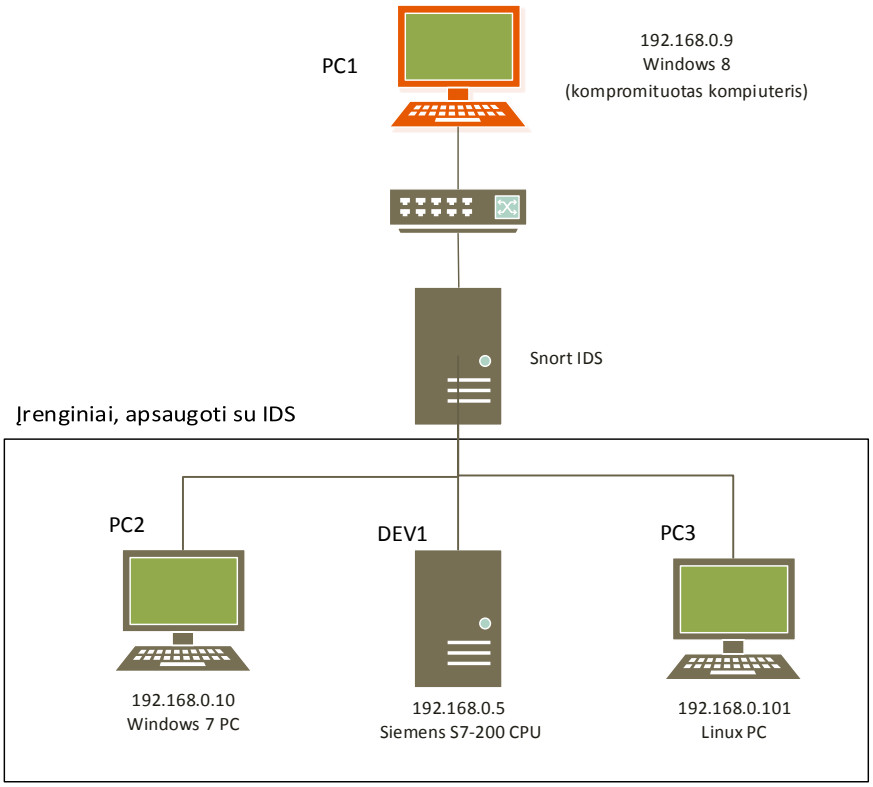
Skenavimo įrankiai

Žvalgybai tinkle bus naudojamas NMAP įrankis ir standartiniai Windows, Linux operacinių sistemų įrankiai „ping“. Aktualūs NMAP parametrai:

- -sP – skenavimas siunčiant tik ICMP ECHO paketus;

- -sS – skenavimas siunčiant vieną SYN paketą į atitinkamus IP adresus;
- -T[0-5] - skenavimo greitis nuo ilgiausio iki greičiausio;
- -sT – sujungimas su sistema SYN – SYN ACK – ACK principu sudarant pilną sesiją;
- -p - pasirenkamas prievadas.

Windows kompiuteris su IP adresu 192.168.0.99 buvo pasirinktas kaip atakos šaltinis. Likę trys įrenginiai buvo apsaugoti su IDS. Visi įrenginiai sujungti į vieną potinklį 192.168.0.0/24, kurių diagramą galima pamatyti 4.2 pav. Bandymų metu buvo simuliuojamas tipinis darbas su sistemomis.



4.2 pav. Tyrimo aplinka be sensoriaus

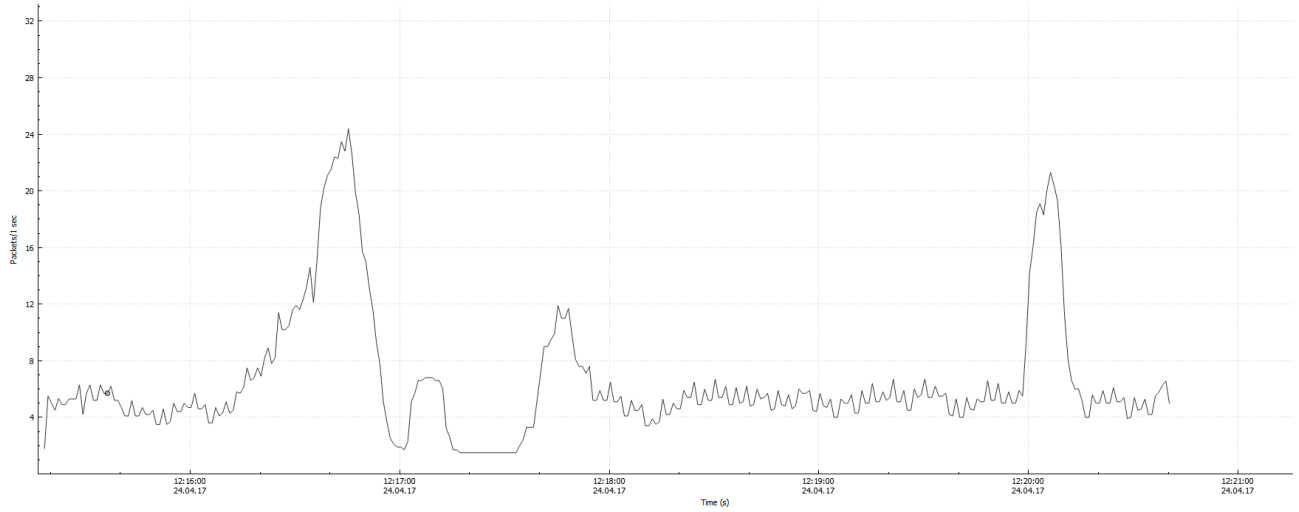
4.3. Pirmasis bandymas: tipinis tinklo skenavimas

Šio bandymo metu bus atlikta tipinė tinklo žvalgyba naudojant NMAP skenavimo įrankį. Veiksmai buvo daromi kiek įmanoma greičiau, nesiekiant išvengti įsilaužimų aptikimo sistemų.

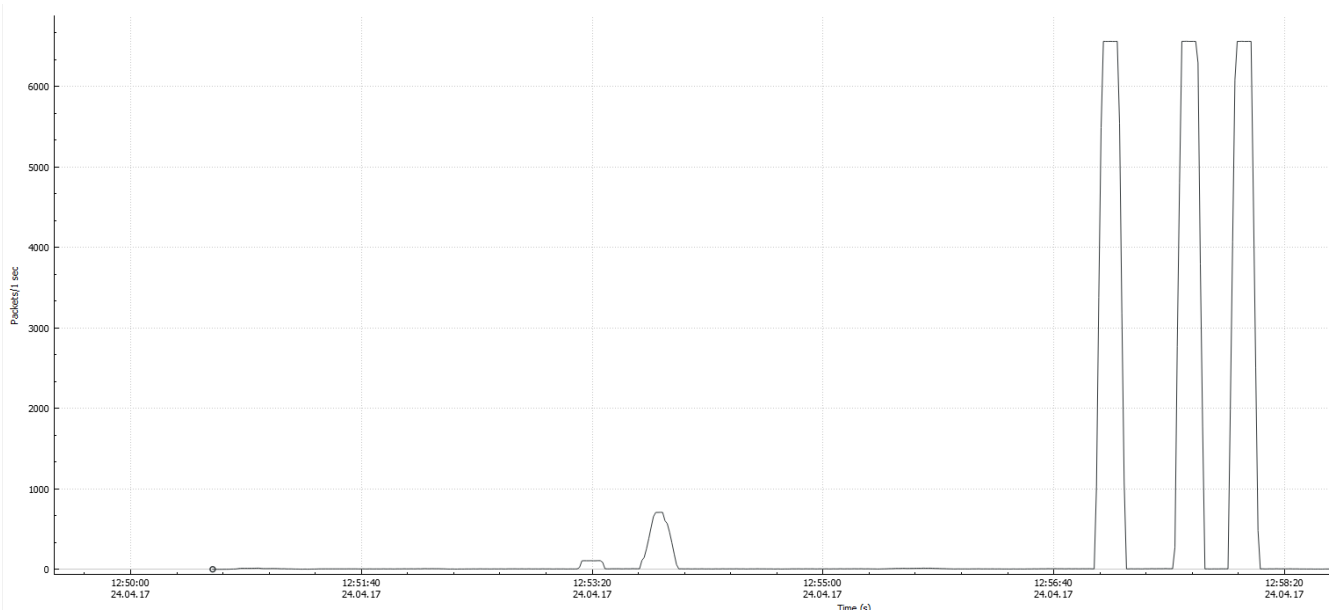
Žingsniai:

1. atliekamas tinklo skenavimas su NMAP naudojant komandą: *nmap -sS 192.168.0.1-254;*
2. pasirenkamos aktyvios sistemos ir suvedamos tokios komandos:
    a. *nmap –sS –p 1-65535 192.168.0.5;*
    b. *nmap –sS –p 1-65535 192.168.0.10;*
    c. *nmap –sS –p 1-65535 192.168.0.101.*

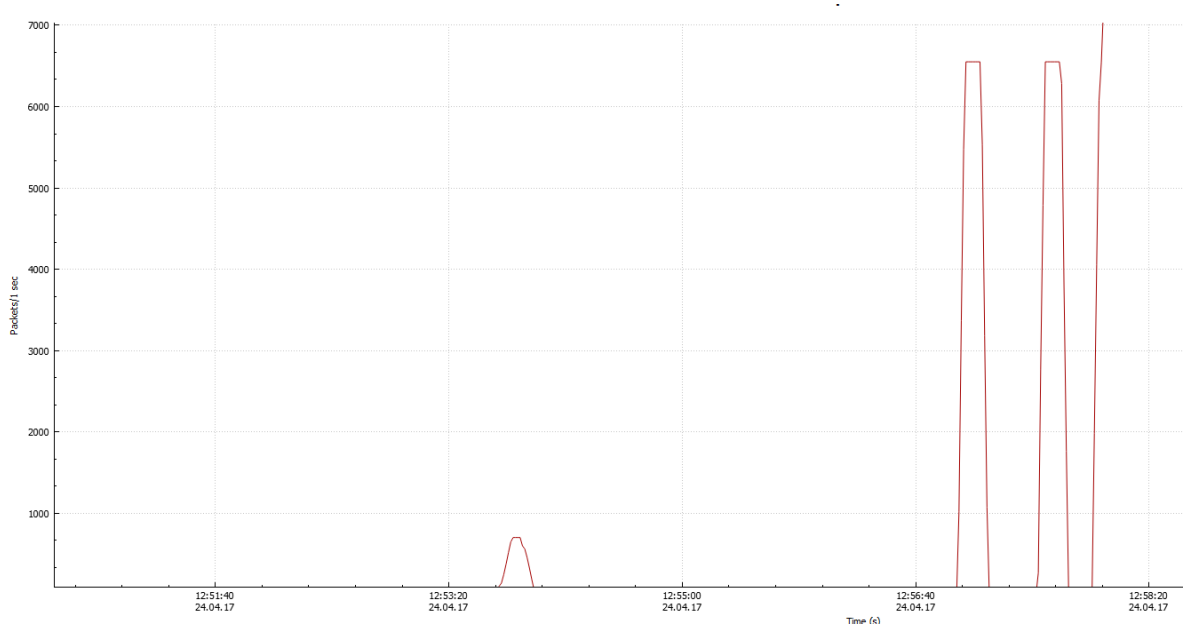
Po atliktų žingsnių buvo surinkta informacija apie potinklyje aktyvias sistemas ir įrenginius, jų preliminarias paskirtis ir pasiekiamus prievadus. Lyginant tinklo srauto diagramas prieš žvalgybą (4.3 pav.) ir jai vykdant (4.4 pav.), iš karto galima pastebėti didžiulį paketų per sekundę šuolį. Jeigu įprastu darbo režimu paketų kiekis svyruoja nuo 6 iki 25 per sekundę, tai žvalgybos metu jų skaičius viršija 6000 per sekundę.



4.3 pav. Srautas tinkle prieš žvalgybą



4.4 pav. Tinklo srautas vykdant žvalgybą



4.5 pav. Išskirti žvalgybos paketai iš bendro srauto

Tiek pirmame (4.6 pav.), tiek ir antrame (4.7 pav) žingsniuose IDS aptiko atliekamus skenavimo veiksmus ir jų šaltinį.

```
04/24-12:53:47.205014  [**] [122:1:1] (portscan) TCP Portscan [**] [Classificati
on: Attempted Information Leak] [Priority: 2] {PROTO:255} 192.168.0.9 -> 192.168
.0.5
04/24-12:53:48.579085  [**] [122:5:1] (portscan) TCP Filtered Portscan [**] [Cla
ssification: Attempted Information Leak] [Priority: 2] {PROTO:255} 192.168.0.9 -
> 192.168.0.101
04/24-12:53:48.855843  [**] [122:5:1] (portscan) TCP Filtered Portscan [**] [Cla
ssification: Attempted Information Leak] [Priority: 2] {PROTO:255} 192.168.0.9 -
> 192.168.0.10
```

4.6 pav. Snort pranešimas po pirmojo skenavimo

```
04/24-12:53:47.205014  [**] [122:1:1] (portscan) TCP Portscan [**] [Classification: Attempted Information Leak] [Priority: 2] {PROTO:255} 192.1
68.0.9 -> 192.168.0.5
04/24-12:53:48.579085  [**] [122:5:1] (portscan) TCP Filtered Portscan [**] [Classification: Attempted Information Leak] [Priority: 2] {PROTO:2
55} 192.168.0.9 -> 192.168.0.101
04/24-12:53:48.855843  [**] [122:5:1] (portscan) TCP Filtered Portscan [**] [Classification: Attempted Information Leak] [Priority: 2] {PROTO:2
55} 192.168.0.9 -> 192.168.0.10
04/24-12:55:19.735730  [**] [122:23:1] (portscan) UDP Filtered Portsweep [**] [Classification: Attempted Information Leak] [Priority: 2] {PROTO
:255} fe80::ace6:1fe1:6eae:f0fe -> ff02::c
04/24-12:55:34.689313  [**] [122:23:1] (portscan) UDP Filtered Portsweep [**] [Classification: Attempted Information Leak] [Priority: 2] {PROTO
:255} 192.168.0.10 -> 224.0.0.252
04/24-12:57:04.094377  [**] [122:1:1] (portscan) TCP Portscan [**] [Classification: Attempted Information Leak] [Priority: 2] {PROTO:255} 192.1
68.0.9 -> 192.168.0.5
```

4.7 pav. Snort pranešimas po antrojo skenavimo

Išvados:

Šis bandymas parodė, kad tinklą skenuojant greitais intervalais, apsaugos sistema aptinka ataką ir teisingai sugeneruoja pranešimus.

4.4. Antrasis bandymas: aptikimo išvengimas

Šio bandymo metu buvo atlikta tinklo žvalgyba naudojant NMAP skenavimo įrankį ir komandą „fping“. Veiksmai bus atliekami taip, kad būtų išvengta skenavimo aptikimo ir kuo labiau imituojant

administratoriaus veiksmus su sistemomis. Tylaus skenavimo principas yra siųsti paketus kuo rečiau, su ilgais laiko tarpais tarp jų. Prievadus reikia nurodyti rankiniu būdu ir tikrinti ne daugiau negu penkis per vieną skenavimą. Norint kuo greičiau identifikuoti sistemas, prievadus verta rinktis protingai, prioritetą suteikiant patiems populiariausiems, kadangi iš jų galima gauti daugiausiai naudingos informacijos.

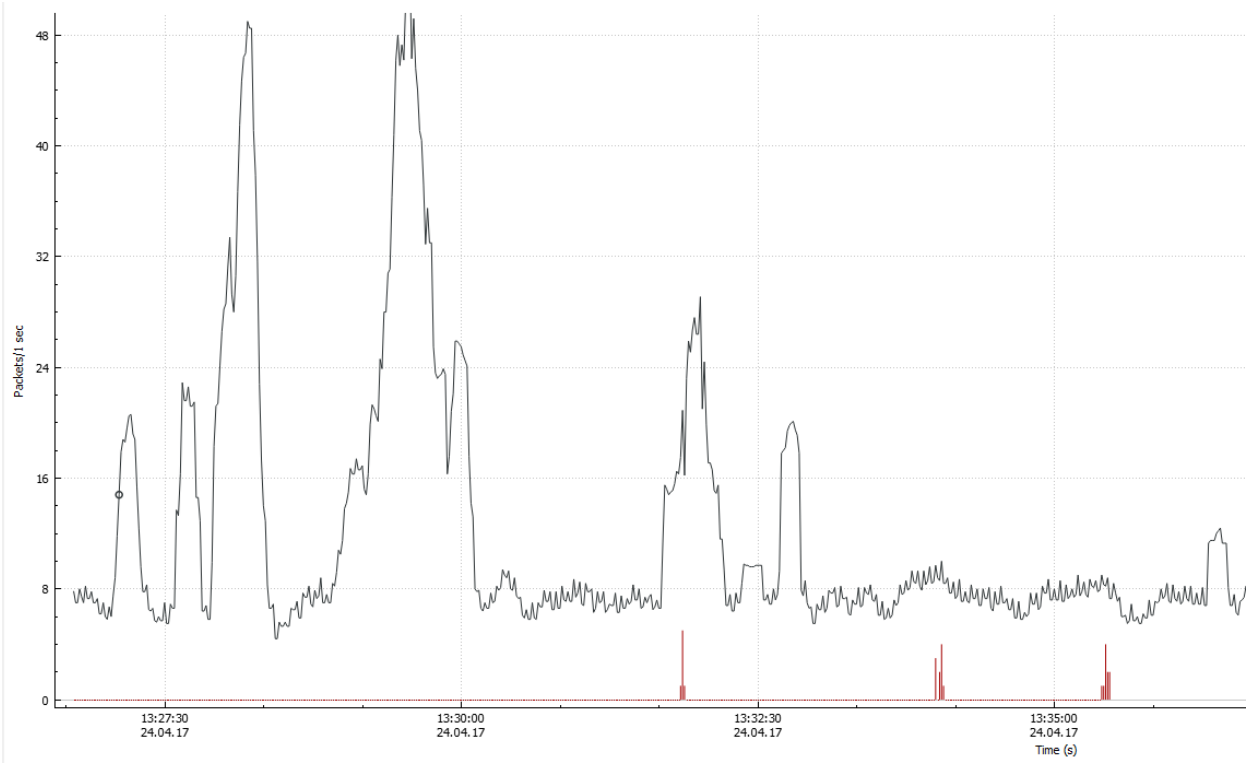
Norint identifikuoti sistemas su žiniatinklio prieiga, galima ieškoti šių atvirų prievadų: 80,443. Norint identifikuoti Windows OS kompiuterius, galima ieškoti šių atvirų prievadų: 137, 139, 445. Norint identifikuoti ICS įrenginius, galima ieškoti šių atvirų prievadų: 502, 19999, 20000.

Žingsniai:

1. atliekama aktyvių įrenginių paieška tinkle naudojant komandą*: fping - g 192.168.0.1-254;*
2. pasirenkamos kelios aktyvios sistemos ir suvedamos tokios komandos:
    a. *nmap –T2 –sS –p 22,80,135,445,443 192.168.0.5;*
    b. *nmap –T2 –sS –p 22,80,135,445,443 192.168.0.10.*
3. po 15 min. laiko tarpo pakartojame komandas, bet su kitais prievadais:
    a. *nmap –T2 –sS –p 21,502 192.168.0.5;*
    b. *nmap –T2 –sS –p 21,502 192.168.0.10.*

Rezultatai

Po atliktų žingsnių buvo surinkta informacija apie potinklyje aktyvias sistemas ir įrenginius. Buvo aptikti ne visi atidaryti prievadai, bet informacijos pakanka norint iš dalies identifikuoti įrenginių paskirtį. Šio bandymo metu IDS neaptiko jokio įlaužimo tinkle. Pažiūrėjus į tinklo srautų diagramą (4.8 pav.), galime pamatyti, kad standartiniame tinklo sraute (juoda linija) yra keletą šuolių, tačiau šiuo atveju jie visiškai nesusiję su skenavimu. Žvalgyba yra išskirta raudona linija, kur mažas paketų kiekis užsimaskuoja bendrame paketų sraute. Dėl to IDS algoritmai neaptiko šių veiksmų kaip tinklo skenavimo.



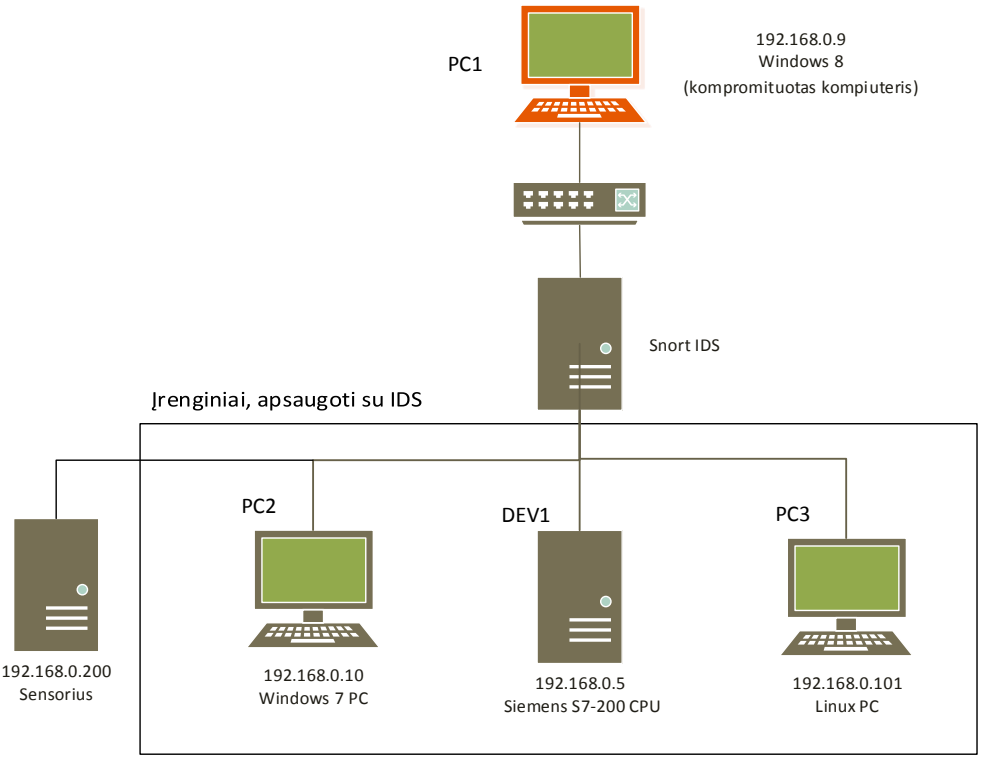
4.8 pav. Tinklo srautas antro bandymo metu

Išvados:

Šis bandymas parodė, kad tinklą skenuojant lėtai galima apeiti apsaugos sistemas, nes paketai pasislepia bendrame sraute, o jų retumas apgauna prievadų skenavimo algoritmus. Šio bandymo metu nebuvo aptikti visi atviri prievadai, bet skenavimą tęsiant tokiu pat principu galima gauti identiškus rezultatus kaip per pirmąjį bandymą. Darant keliolikos minučių tarpus tarp skenavimų, IDS nebegali efektyviai aptikti įsilaužimų, nes sistema stebi IP adresą tam tikrais intervalais, kurie priklauso nuo įsilaužimų aptikimo sistemos ir jos algoritmų konfigūracijos.

4.5. Trečiasis bandymas: skenavimas, kai sensorius yra tinkle

Šis bandymas yra skirtas pademonstruoti siūlomo sprendimo veikimą, darant tuos pačius žingsnius, atliktus antrojo bandymo metu. Prie testuojamos aplinkos buvo prijungtas sensorius. Atnaujintą tinklo topologiją galima pamatyti 4.9 pav.



4.9 pav. Tyrimo aplinka su sensoriumi

Žingsniai

1. atliekama aktyvių įrenginių paieška tinkle su komanda*: fping - g 192.168.0.1-254;*
2. pasirenkamos aktyvios sistemos ir suvedamos tokios komandos:
    a. *nmap –T2 –sS –p 20,80,137,139,21 192.168.0.5;*
    b. *nmap –T2 –sS –p 20,80,137,139,21 192.168.0.10;*
    c. *nmap –T2 –sS –p 20,80,137,139,21 192.168.0.200.*

Rezultatai

Po atliktų žingsnių sensorius sugeneravo pranešimą apie aptiktą anomaliją tinkle, o standartinė IDS sistema žvalgybos veiksmų neaptiko. Pirmojo žingsnio metu buvo gautas pranešimas (4.10 pav.) apie aptiktą vieną ICMP paketą ir informaciją apie paketo šaltinį, šiuo atveju kompromituotą PC1 įrenginį su IP adresu 192.168.0.9 . Kadangi sensorius buvo aptiktas kaip aktyvus įrenginys pirmojo skenavimo metu, jis taip pat buvo skenuotas antrą kartą, siekiant imituoti veiksmus, kuriuos atliktų įsilaužėlis, turėdamas informaciją po pirmojo žingsnio. Sensorius tiksliai aptiko ir sugeneravo įspėjimą apie aptiktus TCP tipo paketus (4.11 pav). Pranešimuose buvo nurodyti 21, 80, 137, 139, 22 prievadai ir šaltinis - įrenginys su IP adresu 192.168.0.9.

```
04/24-14:03:48.059917  [**] [1:10000001:1] Aptiktas ICMP paketas [**] [Classification: Attempted Information Leak] [Priority: 2] {ICMP} 192.168
.0.9 -> 192.168.0.200
```

4.10 pav. Sensoriaus pranešimas pirmojo skenavimo metu

```
.9:33898 -> 192.168.0.200:22
04/24-14:06:02.512009  [**] [1:10000002:1] Aptiktas TCP paketas [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0
.9:33898 -> 192.168.0.200:22
04/24-14:06:02.918298  [**] [1:10000002:1] Aptiktas TCP paketas [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0
.9:33898 -> 192.168.0.200:139
04/24-14:06:03.319639  [**] [1:10000002:1] Aptiktas TCP paketas [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0
.9:33898 -> 192.168.0.200:80
04/24-14:06:03.720549  [**] [1:10000002:1] Aptiktas TCP paketas [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0
.9:33898 -> 192.168.0.200:21
04/24-14:06:04.122282  [**] [1:10000002:1] Aptiktas TCP paketas [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.0
.9:33898 -> 192.168.0.200:137
```

4.11 Sensoriaus pranešimas antrojo skenavimo metu

Išvados

Šis bandymas parodė, kad 3.0 skyriuje siūlomas sprendimas aptinka potinklio žvalgybos veiksmus ir jos algoritmai veikia tiksliai, kaip aprašyta. Turint tokį sensorių atitinkamuose tinklo segmentuose, galima padidinti tikimybę aptikti įsilaužimą ar potencialiai įtartiną veiką tinkle ir ankščiau imtis veiksmų iškilusiai grėsmei suvaldyti.

4.6. Ketvirtasis bandymas: skirtingi skenavimo metodai

Siekiant identifikuoti sensoriaus trūkumus, bandymo metu buvo atliktas skenavimas, naudojant įvairius skenavimo metodus su NMAP įrankiu ir keičiant šaltinio IP adresą. Rezultatus galima pamatyti 4.1 lentelėje.

4.1 lentelė Skirtingų skenavimo metodų rezultatai

Skenavimo metodas	Rezultatas
Ping	+ Aptiko
ARP	- Neaptiko
TCP SYN	+ Aptiko
TCP connect	+ Aptiko
UDP	+ Aptiko
SCTP INIT	- Neaptiko
TCP NULL	+ Aptiko
FIN	+ Aptiko
Xmas	+ Aptiko
TCP ACK	+ Aptiko
TCP Window	+ Aptiko
IP protocol	+ Aptiko

Išvados

Sprendimas aptiko 10 iš 12 skenavimo metodų. Jis negali aptikti skenavimo siunčiant ARP pranešimus, kadangi tokius paketus nuolat siunčia ir gauna visi potinklyje esantys įrenginiai. Sprendimas taip pat neaptinka SCTP paketų, kadangi šis protokolas neparemtas nei TCP, nei UDP principu. Tačiau šiais abiem avejais negalima gauti jokios sistemą identifikuojančios informacijos.

4.7. Tyrimo rezultatai ir pastabos

Apibendrintus visų bandymų rezultatus galima pamatyti 4.2 lentelėje.

4.2 lentelė Tyrimų rezultatai

Veiksmas	Snort IDS	Sensorius
Pirmasis bandymas	+ Aptiko	Nedalyvavo
Antrasis bandymas	- Neaptiko	Nedalyvavo
Trečiasis bandymas	- Neaptiko	+ Aptiko
Ketvirtasis bandymas	Nedalyvavo	Aptiko 10 iš 12 skenavimo metodų

Šio tyrimo metu buvo parodyta, jei žvalgyba tinkle atliekama lėtai, negeneruojant didžiulių paketų srautų ir atliekant veiksmus, kurie artimi administratoriaus veiksmams, galima išvengti būti aptiktiems IDS. Šią saugumo riziką galėtų sumažinti sensorius, kuris generuoja įspėjimus apie jį pasiekiančius paketus. Skirtingai nuo Snort IDS, sensorius yra atsparus laiko atakomis. Tačiau atsisakyti standartinių IDS įrankių negalima, kadangi IDS saugo sistemas tiesiogiai, o siūlomas sensorius saugo netiesiogiai. Sensorius galėtų veikti kartu su kitomis apsaugos sistemomis, padidindamas tikimybę aptikti įsilaužimą ar potencialiai įtartiną veiką tinkle. Jeigu žvalgybos metu piktavalis nesiųs paketų į sensoriaus IP adresą, tokia veikla nebus aptikta.

5. DARBO IŠVADOS

1. Atsiradus verslo poreikiui sujungti technologinius tinklus su korporatyviniais tinklais, šiuolaikinės pramonės valdymo sistemos tampa vis labiau pažeidžiamos, nes telekomunikacijų tinklų ir sistemų pažeidžiamumai kelia grėsmę pramonės tinklams ir sistemoms.
2. Standartiniuose IT tinkluose naudojamos įsilaužimų aptikimo sistemos nesugeba aptikti visų atakų, kuriomis bandoma įsibrauti į pramoninius tinklus. Signatūromis paremtos IDS gali tik iš dalies apsaugoti technologinius tinklus, nes atakų signatūros pramonės sistemoms nėra taip aktyviai kuriamos, kaip standartinėms IT sistemoms. Anomalijų aptikimo sistemos yra sudėtingi, daug kaštų reikalaujantys sprendimai ir yra skirti aptikti sistemų veikimo nuokrypius nuo standartinių modelių, kuomet jos yra paveiktos piktavalio.
3. Norint atskirti įsilaužėlio veiksmus nuo autorizuotų administratoriaus veiksmų, arba aptikti viruso plitimą tinkle, reikia ieškoti šiems įsilaužimams būdingo bruožo – tinklo žvalgybos.
4. Agresyvius tinklo įrenginių skenavimus aptinka standartinės įsilaužimų aptikimo sistemos, tačiau jos yra neatsparios laiko atakoms ir šaltinio keitimo atakomis.
5. Siūlomas metodas gali būti realizuotas panaudojant atviro kodo sistemas, todėl sprendimas nereikalauja didelių investicijų.
6. Įdiegus šią sistemą kartu su kitomis įsilaužimų aptikimo sistemomis, padidėja tikimybė laiku aptikti įsilaužimą ar potencialiai įtartiną veiką tinkle ir skubiai imtis veiksmų iškilusiai grėsmei suvaldyti.
7. Bandymų rezultatai parodė, kad sprendimas yra atsparus laiko atakoms ir šaltinio keitimo atakomis, nes jo principas yra reaguoti ir pranešti apie visus bandymus prisijungti, kurių negali aptikti Snort įrankis.
8. Atliekant tyrimus nustatyta, kad siūlomas spredimas aptinka 10 iš 12 skenavimo metodų.

LITERATŪRA

[1] K. Stouffer, J. Falco ir K. Scarfone, „Guide to industrial control systems (ICS) security," *NIST special publication,* t. 800, pp. 16-16, 2011.

[2] D. Barr, „Supervisory Control and Data," 2004. [Tinkle]. Available: https://scadahacker.com/library/Documents/ICS_Basics/SCADA%20Basics%20-%20NCS%20TIB%2004-1.pdf.

[3] „Cyber Security for SCADA Systems," 2013. [Tinkle]. Available: https://www.thalesgroup.com/sites/default/files/asset/document/thales-cyber-security-for-scada-systems.pdf. [Kreiptasi 14 05 2017].

[4] A. Nicholson, S. Webber, S. Dyer, T. Patel ir H. Janicke, „SCADA security in the light of Cyber-Warfare," *Computers \& Security,* t. 31, pp. 418-436, 2012.

[5] N. Falliere, L. O. Murchu ir E. Chien, „W32. stuxnet dossier," *White paper, Symantec Corp., Security Response,* t. 5, 2011.

[6] D. Kushner, „The real story of stuxnet," *ieee Spectrum,* t. 3, pp. 48-53, 2013.

[7] R. M. Lee, M. J. Assante ir T. Conway, „Analysis of the cyber attack on the Ukrainian power grid," *SANS Industrial Control Systems,* 2016.

[8] robertmlee, „Potential Sample of Malware from the Ukrainian Cyber Attack Uncovered," 01 01 2016. [Tinkle]. Available: https://ics.sans.org/blog/2016/01/01/potential-sample-of-malware-from-the-ukrainian-cyber-attack-uncovered. [Kreiptasi 14 05 2017].

[9] R. E. Mahan, J. R. Burnette, J. D. Fluckiger, C. A. Goranson, S. L. Clements, H. Kirkham ir C. Tews, „Secure data transfer guidance for industrial control and SCADA systems," *Pacific Northwest National Lab (PNNL) Report, http://www. pnnl. gov/main/publications/external/technical reports/PNNL-20776. pdf,* 2011.

[10] „Communication network dependencies for ICS/SCADA Systems," 2016. [Tinkle]. Available: https://www.enisa.europa.eu/publications/ics-scada-dependencies. [Kreiptasi 14 05 2017].

[11] V. M. Igure, S. A. Laughter ir R. D. Williams, „Security issues in SCADA networks," *Computers \& Security,* t. 25, pp. 498-506, 2006.

[12] Symantec, „Internet Security Threat Report," 04 2016. [Tinkle]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf. [Kreiptasi 14 05 2017].

[13] O. Andreeva, S. Gordeychik, G. Gritsai ir O. Kochetova, „INDUSTRIAL CONTROL SYSTEMS VULNERABILITIES STATISTICS," 2016. [Tinkle]. Available: https://kasperskycontenthub.com/securelist/files/2016/07/KL_REPORT_ICS_Statistic_vulnerabilities.pdf. [Kreiptasi 14 05 2017].

[14] S. East, J. Butts, M. Papa ir S. Shenoi, „A Taxonomy of Attacks on the DNP3 Protocol," įtraukta *International Conference on Critical Infrastructure Protection*, 2009.

[15] B. Zhu, A. Joseph ir S. Sastry, „A taxonomy of cyber attacks on SCADA systems," įtraukta *Internet of things (iThings/CPSCom), 2011 international conference on and 4th international conference on cyber, physical and social computing*, 2011.

[16] A. Čenys ir J. Juknius, Saugumo patikros ir etiško įsilaužimo technologijos, TEV, 2011, pp. 20-62.

[17] K. Scarfone ir P. Mell, „Guide to intrusion detection and prevention systems (idps)," *NIST special publication*, t. 800, p. 94, 2007.

[18] T. H. Ptacek ir T. N. Newsham, „Insertion, evasion, and denial of service: Eluding network intrusion detection," 1998.

[19] V. Bukac, „IDS system evasion techniques," *Master. Masarykova Univerzita*, 2010.

[20] Z. Jammes ir M. Papadaki, „Snort IDS Ability to Detect Nmap and Metasploit Framework Evasion Techniques," *Advances in Communications, Computing, Networks and Security Volume 10*, p. 104, 2013.

[21] D. G. Peterson, „Quickdraw Architecture – Snort Additions," 2008. [Tinkle]. Available: http://www.digitalbond.com/blog/2008/10/27/quickdraw-architecture-snort-additions/.

[22] S. Amin, X. Litrico, S. Sastry ir A. M. Bayen, „Cyber security of water SCADA systems—Part I: Analysis and experimentation of stealthy deception attacks," *IEEE Transactions on Control Systems Technology*, t. 21, pp. 1963-1970, 2013.

[23] P. Düssel, C. Gehl, P. Laskov, J.-U. Bußer, C. Störmann ir J. Kästner, „Cyber-critical infrastructure protection using real-time payload-based anomaly detection," įtraukta *International Workshop on Critical Information Infrastructures Security*, 2009.

[24] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner ir A. Valdes, „Using model-based intrusion detection for SCADA networks," įtraukta *Proceedings of the SCADA security scientific symposium*, 2007.

[25] A. Valdes and S. Cheung, "Communication pattern anomaly detection in process control systems," in *Technologies for Homeland Security, 2009. HST'09. IEEE Conference on*, 2009.

[26] I. N. Fovino, M. Masera, M. Guglielmi, A. Carcano and A. Trombetta, "Distributed intrusion detection system for SCADA protocols," in *International Conference on Critical Infrastructure Protection*, 2010.

[27] D. Chiarella, „WORM DETECTION: a monitoring behaviour based system," 2006.

[28] „ICS/SCADA honeypot,“ [Tinkle]. Available: https://github.com/mushorg/conpot. [Kreiptasi 14 05 2017].