Lietuvos mokslo ir studijų institucijų kompiuterių tinklas LITNET

Vilniaus universitetas

Ankstyvo perspėjimo apie grėsmes paslauga

Paslaugos aprašymas

Paslauga sukurta vykdant Europos socialinio fondo finansuojamą projektą „Mokslo ir studijų institucijoms LITNET teikiamų IT paslaugų plėtra“ Nr. 09.3.3-ESFA-V-711-01-0003

Kuriame Lietuvos ateitį

2014–2020 metų Europos Sąjungos fondų investicijų veiksmų programa

Vilnius

2018 m.

Kompiuterių tinkluose naudojamos įvairios techninės priemonės jų saugumui užtikrinti. Tarp jų populiariausios užkardos (angl. firewall), atakų aptikimo ir prevencijos sistemos (angl.intrusion detections & prevention sustem, IDPS) paprastai atlieka vieną specializuotą funkciją ir visos kartu didina informacijos apsikeitimo tinkle saugumą. „Honeypot“ sprendimai (toliau – sensoriai) nuo tradicinių priemonių skiriasi tuo, kad leidžia ne tik aptikti ir sustabdyti atakas, bet tai daroma tikslingai nukreipiant įsilaužėlio dėmesį į save – imituojant pažeidžiamas tarnybas ar netikrus kompiuterių tinklus.

Ankstyvo perspėjimo apie grėsmes sistema (toliau APGS) yra skirta aptikti kenkėjišką veiklą tinkle ir jos prevencijai. LITNET tinkle statomi sensoriai, kuriuose veikia paslaugas (SSH, Web ir kt.) imituojančios tarnybos, IDS programinė įranga. Sensorių renkama informacija apie atakas, prievadų skenavimus ir visus į juos nukreiptus įvykius, siunčiama į centrinį serverį, kur yra apdorojama, klasifikuojama ir perduodama galiniams naudotojams. Tai bus sistemų, tinklų administratoriai, kurių tinkle bus statomi sensoriai. Administratoriai turės galimybę aprašyti filtrus pagal juos dominančius įvykius ir gauti atitinkančių IP adresų sąrašą, kurį galės panaudoti rankiniu ar automatiniu būdu blokuoti kenkėjus savo tinkle. Paslaugos tikslas yra LITNET tinklo mastu fiksuoti kenkėjišką veiklą ir dalintis šia informacija tarpusavyje.

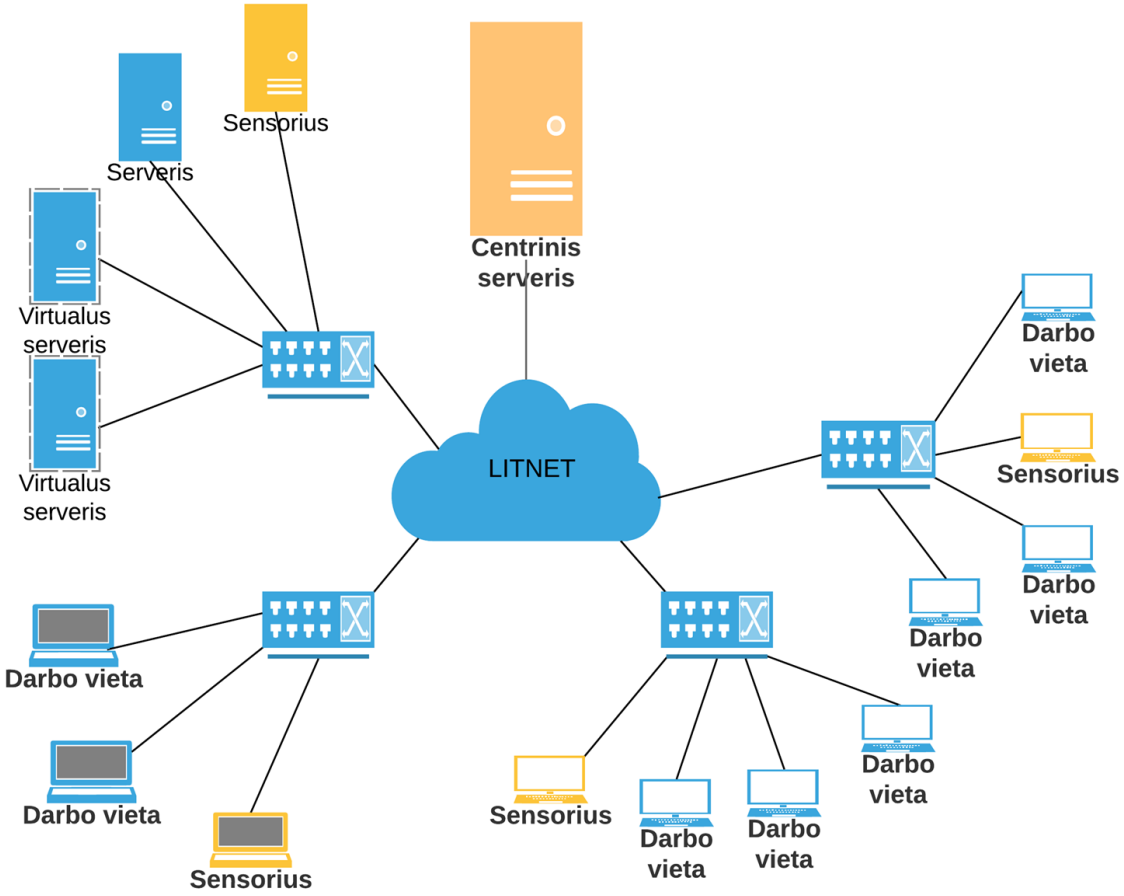
Paslaugos naudotojai yra tinklo administratoriai.

Sensoriai gali suteikti papildomos informacijos apie tinkle vykstančius procesus. Kiekvieną dieną iš apsaugos ir paslaugų mechanizmų yra surenkamas didelis kiekis duomenų, dažnai yra sunku atskirti „gerus“ įvykius nuo „blogų“. Sensorių sistema yra skirta tik įsilaužimams stebėti, todėl surenkamų duomenų kiekis yra daug mažesnis ir didžioji dalis jų yra iš atakuotojų.

Kita priežastis kodėl reikėtų savo tinkle naudoti sensorių sistemą: nedidelis resursų sunaudojimas, diegimo paprastumas, vertės įrodymas. Bet kokia saugumo priemonė turi vertę organizacijoje, tačiau ne visuomet akivaizdu, pavyzdžiui, tinkamai suderinta užkarda praktiškai nepastebima kasdieniame tinklo infrastruktūros gyvenime, todėl atsiranda netikro saugumo jausmas – atrodo, jog mūsų tiesiog nepuola, o jeigu ir puola, tai negali apeiti užkardos. Organizacijos viduje įrengto sensoriaus įvykių registracijos žurnalai gali pademonstruoti grėsmės egzistavimą ir padėti pagerinti naudojamų techninių priemonių kokybę.

Sistemos veikimo principas

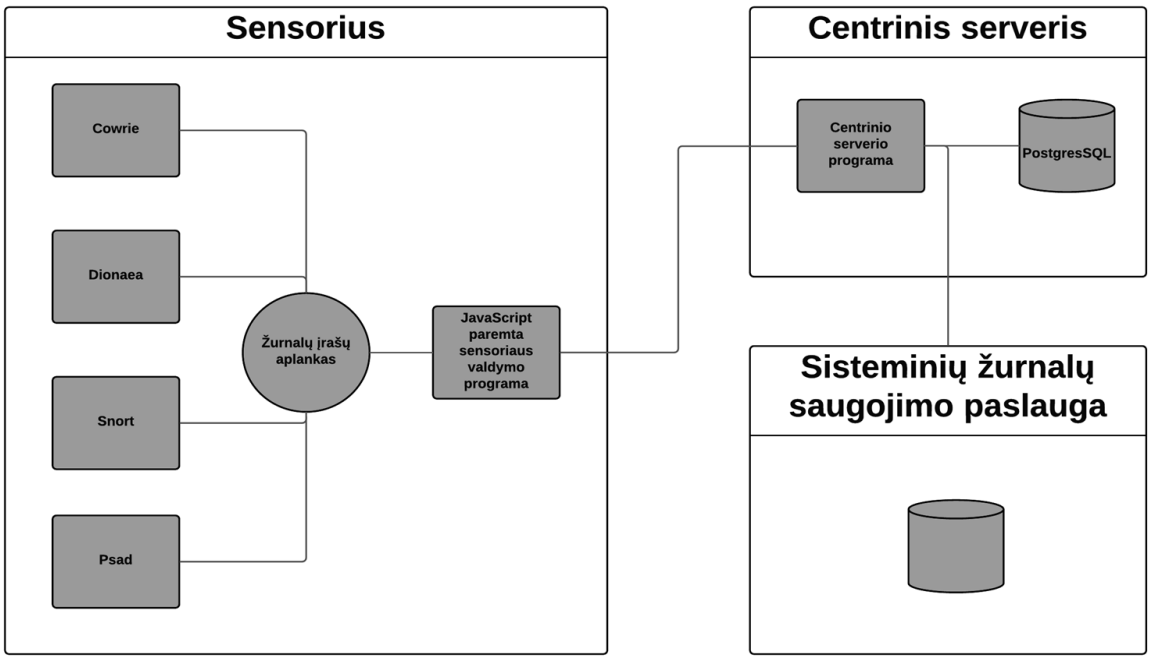
1. Sensorių tinklas ir informacijos surinkimas



Pav. 1 Sensorių tinklas

Įvairiose LITNET tinklo vietose statomi sensoriai renka informaciją apie atakuotojus ir siunčia į centrinį serverį (1 pav.). Ryšis su centriniu serveriu inicijuojamas sensoriaus ir sukuriama sesija. Šiuo kanalu sensorius siunčia informaciją apie kenkėjišką veiklą ir gauna nustatymus, komandas iš centrinio serverio.

Iš sensoriuose naudojamų programų surinkti žurnalų įrašai įkeliami į PostgreSQL duomenų bazę, taip pat išsaugomi į syslog, iš kurio yra siunčiami į žurnalų įrašų saugojimo serverį (2.3.1 veikla).



Pav. 2 Žurnalų įrašų surinkimas

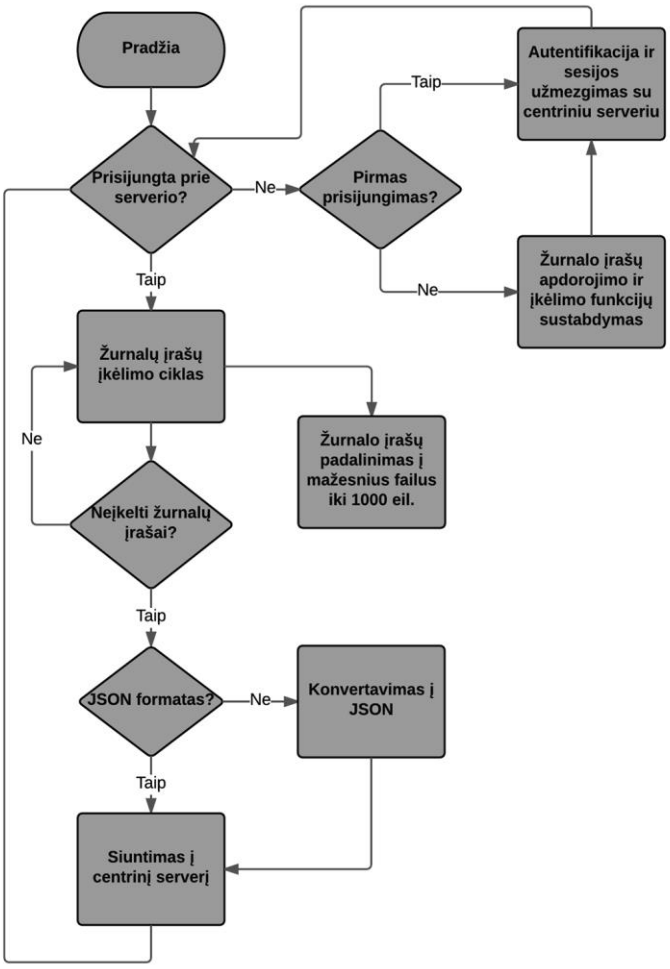
2. Sensoriai ir centrinis serveris

Sensoriuose pažeidimams aptikti naudojamos 5 programos:

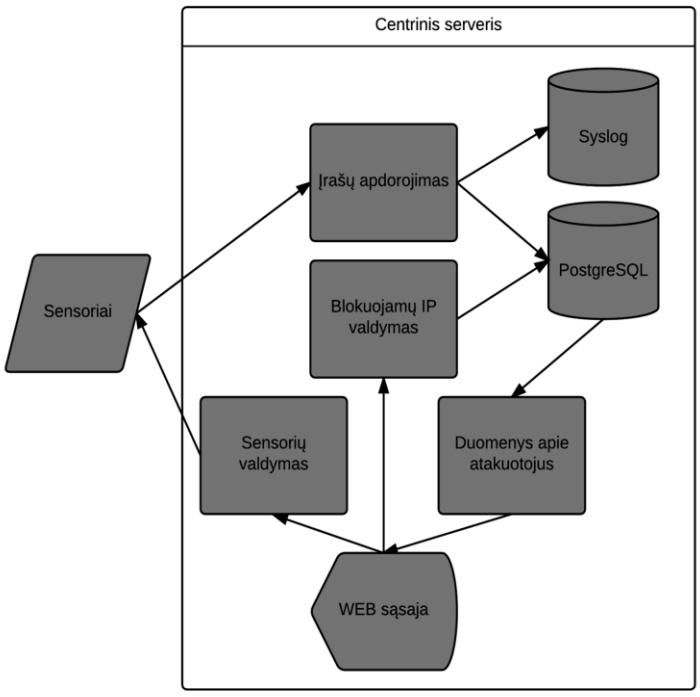
- Cowrie – SSH ir Telnet imitacija;
- Dionaea – įvairių paslaugų su pažeidžiamumais imitacija (HTTP, HTTPS, MYSQL, MSSQL);
- Snort – įsibrovimų aptikimo ir prevencijos sistema;
- Psad – prievadų skenavimų aptikimas;
- HoneyD – virtualių kompiuterių imitavimas, srauto iš jų nukreipimas į sensorių.

Sensoriuose veikiančios žurnalų įrašų apdorojimo ir prisijungimo tarnybos veikimo principas parodytas 3 pav. Ši tarnyba surenka visų kenkėjišką veiklą stebinčių programų įrašus, juos apdoroja ir siunčia į centrinį serverį. Centriniame serveryje šie įrašai surenkami ir įkeliami į duomenų bazę (4 pav.). Sensorių stebėjimas ir valdymas vykdomas per web sąsają. Prieiga prie serverio yra autorizuota, naudotojų duomenys tikrinami su SSO. Pagrindinės web sąsajos funcijos yra:

- Leisti administratoriams stebėdi savo tinkle pastatytus sensorius ir jų siunčiamus įspėjimus;
- Valdyti sensoriuose veikiančias kenkėjiškos veiklos aptikimo programas;
- Nurodyti, kurie IP adresai bus įtrauki į blokuojamų IP adresų lentelę, individualiai arba pagal įspėjimo rūšį.



Pav. 3 Sensoriaus tarnyba



Pav. 4 Centrinis serveris

3. Techninės specifikacijos

3.1. Serveris

Parametro pavadinimas	Parametras/versija
Programinė įranga	
Operacinė sistema	Ubuntu Server 16.04 LTS
HTTP serveris	Apache/2.4.7 ar aukštesnė
Duomenų bazė	PostgreSQL 9.5 ar aukštesnė
PHP variklis	PHP 7.0.8 ar aukštesnė
JavaScript variklis	Node.js v6.9.2 ar aukštesnė
Web aplikacijų kūrimo sistema	JQWidgets 4.5.0 ar aukštesnė
Aparatinė įranga	
Procesorius	2 branduoliai po 2 GHz ar daugiau
Operatyvioji atmintis	2 GB ar daugiau
Tinklo kortos pralaidumas	1 Gbps ar daugiau
Kietojo disko talpa	200 GB ar daugiau

Lentelė 1. Serverio parametrai

3.2. Sensoriai

Kiekis – 320 vnt.

Parametro pavadinimas	Parametras/versija
Programinė įranga	
Operacinė sistema	Raspbian Jessie Lite 2017-01-15
Snort	Snort 2.9.7.0 ar aukštesnė
Psad	Psad 2.2.3 ar aukštesnė
Dionaea	Dionaea 2014-06-26 ar aukštesnė
Cowrie	Cowrie 1.1.0 ar aukštesnė
HoneyD	Honeyd 1.5c ar aukštesnė
JavaScript variklis	Node.js v6.9.2 ar aukštesnė
Aparatinė įranga	
Procesorius	4 branduoliai po 1 GHz ar daugiau
Operatyvioji atmintis	1 GB ar daugiau
Tinklo kortos pralaidumas	100 Mbps ar daugiau
Atminties kortelės talpa	16 GB ar daugiau

Lentelė 2. Sensorių parametrai