Lietuvos mokslo ir studijų institucijų kompiuterių tinklas Litnet

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Vilniaus Gedimino technikos universitetas

Automatinio saugumo audito paslauga

Paslaugos aprašas

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

TURINYS

Įvadas

Lietuvos mokslo ir studijų institucijų kompiuterių tinklas LITNET (toliau – LITNET) jungia mokslo ir studijų institucijų (toliau – MSI) kompiuterių tinklus. Prie šio tinklo prijungtoms institucijoms teikiamos duomenų perdavimo paslaugos, diegiami inovatyvūs kompiuterių tinklo ir paslaugų sprendimai. LITNET infrastruktūrą valdo ir tinklo paslaugas teikia LITNET techniniai centrai.

Kompiuterių tinklo saugumui užtikrinti yra įkurta LITNET tinklų ir informacijos saugumo incidentų reagavimo tarnyba (LITNET CERT). LITNET CERT kartu su LITNET techninių centrų atstovais atlieka kompiuterinių incidentų tyrimus, teikia naudotojams konsultacijas tinklo saugumo klausimais, analizuoja kompiuterinio saugumo situaciją LITNET tinkluose ir vykdo kompiuterinių incidentų prevenciją. Tačiau informacijos saugos užtikrinimas nėra paprastas uždavinys, jis reikalauja turėti ir LITNET institucijose nemažai kvalifikuoto personalo, galinčio vykdyti atitinkamas funkcijas ir palaikyti saugią kompiuterinių sistemų būseną. Jei didesnieji universitetai gali tai atlikti savarankiškai, tai mažesnės MSI tokių galimybių neturi. Todėl ši paslauga pirmiausia ir yra skirta į .LITNET tinklą įsijungusių MSI kompiuterių administratoriams, kitiems jų darbuotojams (mokslininkams, tyrėjams) pasitikrinti savo naudojamų kompiuterinių sistemų (serverių, web svetainių) saugumo lygį.

Automatinio saugumo audito paslaugos tikslas yra siekiant centralizuoti informacinių sistemų saugos užtikrinimo uždavinius, optimizuoti investicijas, skirtas informacinių sistemų pažeidžiamumų paieškai ir informacijos saugos auditui, mažinti technologinę ir žinių atskirtį tarp Litnet institucijų, turinčių informacijos saugą užtikrinančius padalinius ir institucijų, turinčių tik minimalų IT aptarnaujantį personalą, mažinti saugos pažeidžiamumų ir saugos incidentų lygį Litnet tinkle, taip prisidėti prie kokybiškesnio paslaugų teikimo ir bendro šalies kibernetinės saugos užtikrinimo, skatinti nekomercinio ir atviro kodo sprendimų taikymą Lietuvos mokslo ir studijų institucijų informacijos saugos sprendimuose.

Paslaugos aprašą sudaro tokios dalys kaip paslaugos taikymo sritys, paslaugos architektūriniai sprendimai, paslaugos funkcionalumas, paslaugos naudotojai, prisijungimas prie paslaugos ir jos užsisakymas, automatinio saugumo audito vykdymas ir gautų rezultatų interpretavimas.

1. Paslaugos taikymo sritys.

Automatinio informacijos saugumo audito paslauga (toliau – AISAP) skirta atlikti pasirinkto serverio ar interneto svetainės informacinio pažeidžiamumo skenavimą ir gauti jo ataskaitą.

2. Paslaugos architektūriniai sprendimai

Paslaugios architektūra yra suprantama kaip informacinės sistemos, įgyvendinančios AISAP paslaugą, komponentų visuma, apimanti tų komponentų (posistemių) tarpusavio sąveikos ir valdymo būdus.

2.1 Loginė paslaugos architektūra

Atsižvelgiant į esamas LITNET informacijos saugos užtikrinimo problemas AISAP architektūra suprojektuota taip, kad tenkintų tokius reikalavimus:

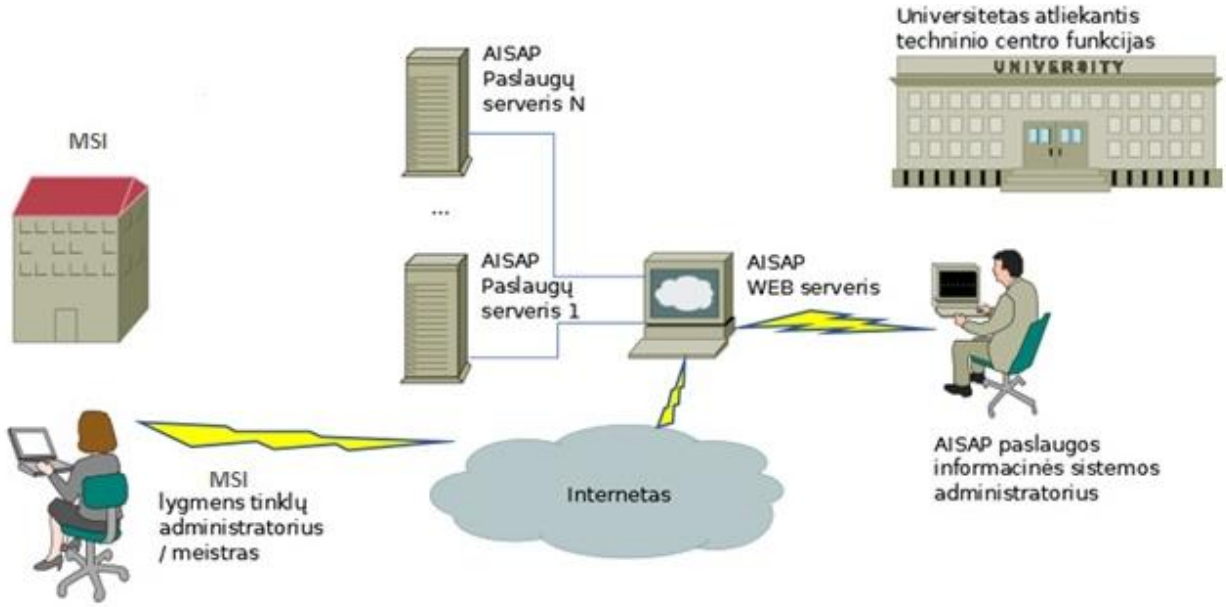
- yra galimybė priskirti paslaugos administravimą pasirinktam techniniam centrui;
- sistemos sukonstruota moduliniu principu, siekiant maksimaliai lanksčiai adaptuotis prie LITNET infrastruktūros įvairovės, numatyti galimybę ateityje plėsti siūlomų informacijos saugos paslaugų spektrą;
- paslauga užtikrina pažeidžiamumą automatinį skenavimą (auditą) kuo platesniam kompiuterinės įrangos spektrui; nesant galimybei realizuoti skenavimą visam įrangos spektrui, yra galimybė integruoti tokį funkcionalumą per integracijos modulį ateityje;
- orientacija į nemokamus atviro kodo sprendimus, siekiant išvengti finansinės priklausomybės nuo įrangos tiekėjo;
- prieigos prie paslaugos užtikrinimas iš naudotojo, naudojančios sąlyginai pasenusią ir riboto galingumo kompiuterinę įrangą, pusės;
- griežta informacijos saugos audito rezultatų apsauga nuo nesankcionuotos peržiūros.

Įvardyti poreikiai susiaurino galimų architektūrinių sprendimų pasirinkimą, todėl pasirinktas hibridinis paslaugos architektūros modelis, turintis kliento-serverio ir komponentų modelio (*angl*. Component-based software engineering (CBSE)) savybėmis:

- kliento-serverio ir CBSE architektūros integracija;

- skaičiavimų / veiksmų koncentracija serverinėje dalyje, siekiant minimizuoti resursų poreikį kliento daliai; kliento dalis – web sąsaja, nereikalaujanti papildomų įskiepių (*angl.* plug-ins);
- nuotolinė prieiga prie serverio per Internet tinklą, nereikalaujanti papildomos įrangos, skirtosios linijos;
- serverinė dalis realizuojama modulinės architektūros principu; prieiga prie atskirų modulių iš kliento pusės realizuojama „vieno langelio“ principu per web-servisus;
- duomenų saugojimas realizuojamas tik serverinėje dalyje; duomenų saugojimas yra atskiriamas loginiais ir aparatiniais sprendimais nuo aplikacinės dalies siekiant maksimizuoti saugomų duomenų saugumą.

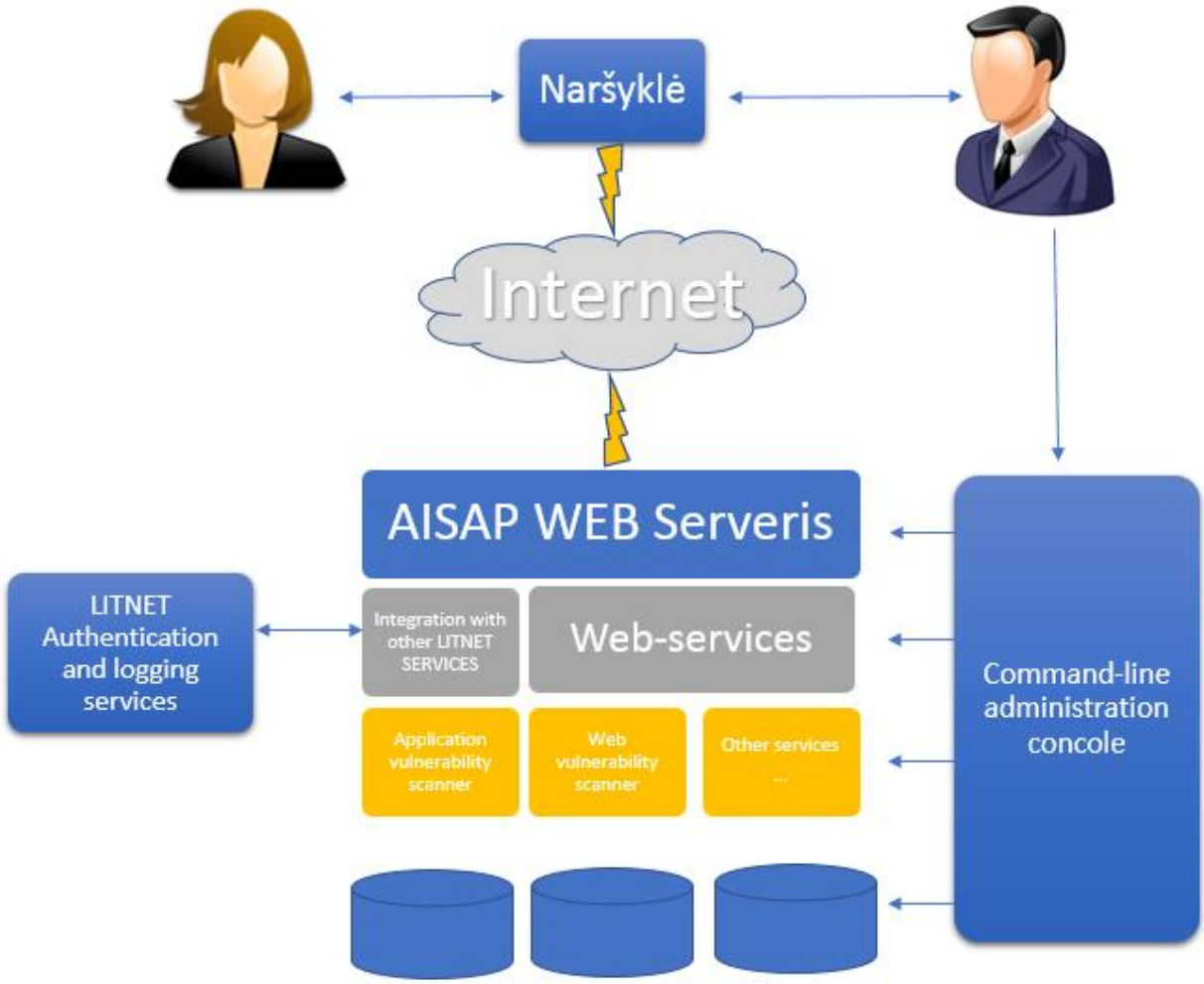
Bendra paslaugos architektūrinė schema pateikta 1 pav.:



1 pav. Bendra AISAP architektūrinė schema

AISAP paslaugos naudotojas jungiasi saugiu kanalu per internetą prie AISAP web serverio naudodamasis interneto naršykle savo kompiuteryje. Prisijungęs prie sistemos jis gali pasirinkti (užsakyti) paslaugas iš skirtingų sistemos siūlomų paslaugų, tokių kaip savo MSI serverio ar interneto svetainės skenavimas. Savo paskyroje naudotojas mato savo sistemų statusą, skenavimų istoriją gali persisiųsti audito ataskaitas. Savo ruožtu AISAP informacinės sistemos administratorius, dirbantis LITNET techniniame centre atlieka AISAP sistemos konfigūravimo ir priežiūros darbus, stebi ir konsultuoja naudotojus, atlieka AISAP sistemos integraciją su kitais moduliais.

2 paveiksle pateikiama AISAP loginė architektūra, aprašanti komponentus ir jų tarpusavio ryšius.



2 pav. AISAP komponentai ir jų loginiai ryšiai

Kaip matyti iš 2 pav. pateiktos AISAP loginės architektūros schemos, sistemą sudaro tokie komponentai:

- Kliento dalis – per web naršyklę atidaroma naudotojo sąsaja, kuri skiriasi galiniam naudotojui ir administratoriui (žr. 3 pav. ir 4 pav.).
- Serverinė dalis – ją sudaro tokie komponentai:
  - AISAP web serveris;
  - WEB servisai;
  - Integracijos su kitomis LITNET sistemomis modulis;
  - Pažeidžiamumų skenavimo moduliai;

- Pažeidžiamumų skenavimo modulių saugyklos

Apibendrinant paslaugos architektūrą, galima išskirti tokius bendruosius AISAP architektūros bruožus:

- AISAP IS sukonstruota vieningą sąsają turinčios integracinės platformos principu, integruojančios šiame etape numatytus, taip pat perspektyvius, atviro kodo ir nekomercinius įrankius.
- Duomenų mainai tarp skirtingų paslaugos modulių vyksta taikant industrijos standartus atitinkančius standartus ir formatus, tokius kaip XML arba analogiškus.
- Integruojami moduliai išlaiko vieningą naudojo sąsają.

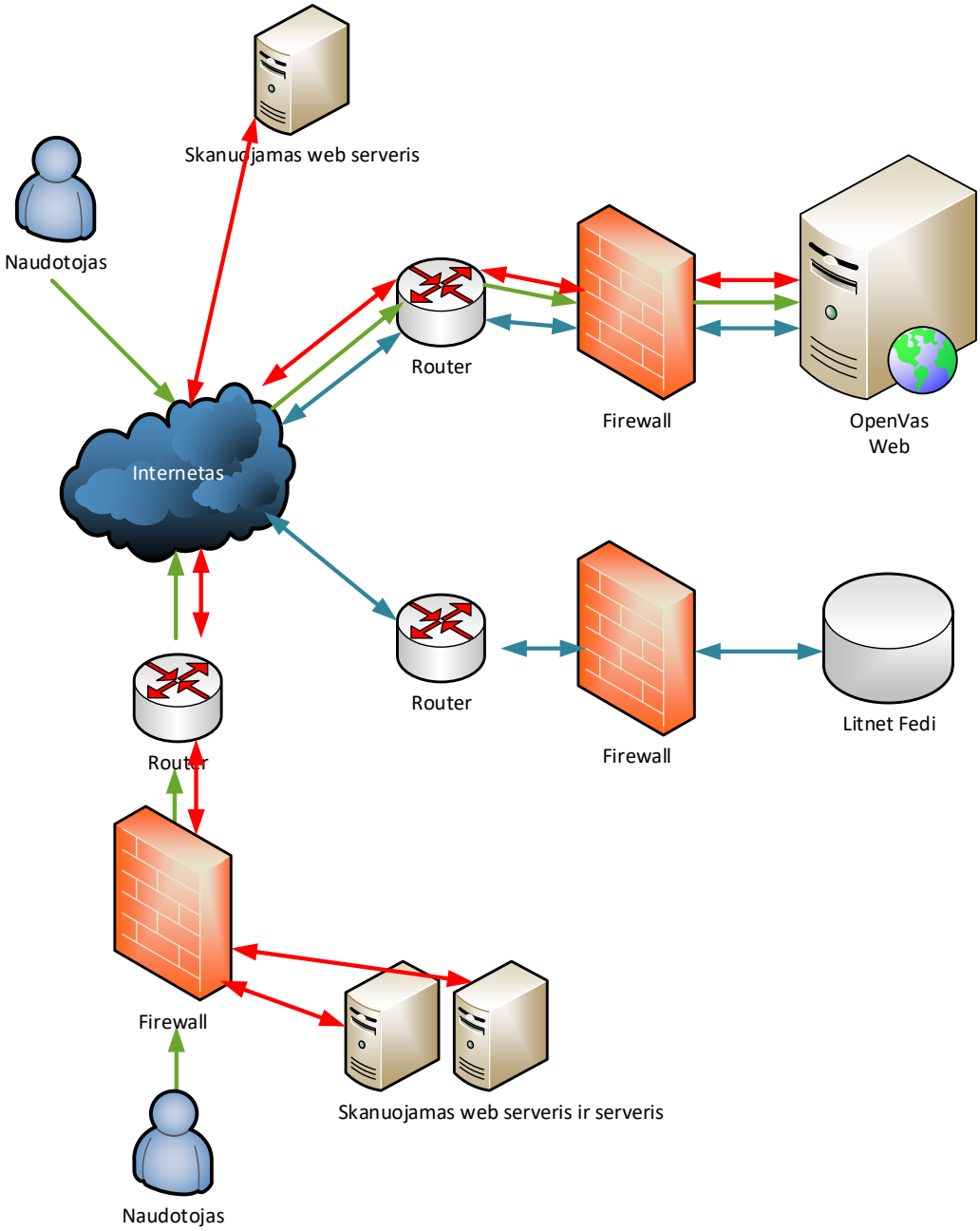
2.2. Fizinė architektūra

Fizinė automatinio saugumo audito paslaugos kliento – serverio tipo architektūra yra pateikta 3 paveiksle:

Pagal siūlomą sistemos loginę architektūrą fizinė paslaugos įranga buvo sumontuota ir įdiegta klasikinėje duomenų centro infrastruktūroje, bet yra galimybė ją įdiegti debesyse (*angl.* Cloud computing), taip neprisirišant prie konkrečios aparatinės realizacijos.

Kaip matoma iš pateiktos 3 paveiksle architektūros schemos, sistema suformuota iš atskirų aparatinių ar virtualių serverių:

- panaudota atviro kodo sistemos (operacinė sistema), kad neatsirastų papildomų išlaidų programinės įrangos licencijų įsigijimui;
- nors schemoje nėra pažymėta, tačiau tuo atveju jei į AISAP sistemą diegiamas / integruojamas komponentas (pvz., pažeidžiamumų skeneris arba WEB serveris), jis gali būti klasterizuojamas;
- įdiegta ugniasienė ir maršrutizatorius, kuris geba atlikti paketų persiuntimą (*angl.* forward) į vidinį resursą, kurio skenavimą reikia atlikti;



3 pav. AISAP fizinė architektūra

2.3. paslaugos saugumo reikalavimų užtikrinimas

AISAP paslauga yra suprojektuota, sukurta ir įdiegta vadovautis standarto ISO/IEC 27001:2013 reikalavimais. ***Bendri saugos reikalavimai*** fizinei AISAP architektūrai:

- paslaugos web serveris patalpintas DMZ zonoje;
- Duomenų bazės ir paslaugų serveriai talpinami apsaugotame vidiniame tinklo segmente, atskirtame nuo DMZ;

- sistemoje saugomi Litnet institucijų atliktų auditų duomenys (tame tarpe apie nustatytus pažeidžiamumus) yra konfidencialūs, t.y. yra užtikrinama, kad ši informacija yra prieinamą tik teisėtiems naudotojams; vienos Litnet institucijos naudotojas nemato kitos institucijos skenavimo rezultatų ir kitų duomenų; Duomenų matomumas ir prieinamumas AISAP naudotojams yra realizuotas ir užtikrintas pagal principą „Tiek kiek būtina ir kiek įmanoma mažiau“.
- reguliariai atliekamas rezervinis duomenų kopijavimas. Archyvinės kopijos saugomos ne trumpiau, nei nustato IS administratorius per konfigūracinius parametrus.
- naudotojų autentifikacija yra užtikrinama per IS autentifikavimo bazės integraciją su Litnet naudotojų autentifikavimo sistema. Autentifikacijos sistema i paveldi visus reikalavimus dėl naudotojų saugos parametrų (pvz., slaptažodžių ilgis, bandymų jungtis skaičius, po kurių vyksta prisijungimo blokavimas ir t.t.).
- saugumo ir kitų įvykių informacija registruojama ir saugoma ne mažiau kaip 12 mėnesių;

3. Paslaugos funkcionalumai

Paslaugos funkcionalumai yra susieti ir priklauso nuo paslaugos naudotojo statuso (galinis naudotojas, paslaugos administratorius) bei paslaugos komponento (web serveris, web servisai, integracijos modulis, pažeidžiamumų skenavimo modulis ir t.t.)

Galinio naudotojo sąsaja turi tokius funkcionalumus:

- Galimybė nustatyti skenavimui IP adresus ir IP adresų blokus arba DNS vardus;
- Galimybė pasirinkti skenavimo tipą (-us) nustatytiems adresams;
- Galimybė pasirinkti skenavimo laiką, nustatant nereguliarius arba periodinius skenavimus, ir jį keisti;
- Galimybė pasirinkti skenavimo intensyvumą – lengvas, normalus, intensyvus;
- Galimybė įvesti ir išsaugoti skenuojamos sistemos prisijungimo duomenis, siekiant atlikti „gilesnį skenavimą“;
- Galimybė sustabdyti skenavimą skenavimo eigoje;

- Galimybė peržiūrėti ir komentuoti (tuo atveju, jei naudotojas mano, kad tai yra klaidingai-teigiamas pranešimas) skenavimo rezultatus, jų istoriją, juos eksportuoti į XLS/PDF/HTML formatus.

AISAP administratoriaus sąsaja turi tokius funkcionalumus:

- Galimybė administruoti naudotojus (kurti, trinti, blokuoti, keisti slaptažodžius, keisti naudotojų informaciją);
- Galimybė nustatyti skenavimui IP adresus ir IP adresų blokus arba DNS vardus;
- Galimybė pasirinkti skenavimo tipą (-us) nustatytiems adresams (taip pat susiejant skenavimą su tam tikru naudotoju);
- Galimybė pasirinkti skenavimo laiką, nustatant nereguliarius arba periodinius skenavimus, ir jį keisti (taip pat susiejant skenavimą su tam tikru naudotoju);
- Galimybė pasirinkti skenavimo intensyvumą – lengvas, normalus, intensyvus (taip pat susiejant skenavimą su tam tikru naudotoju);
- Galimybė įvesti ir išsaugoti skenuojamos sistemos prisijungimo duomenis, siekiant atlikti „gilesnį skenavimą“ (taip pat susiejant skenavimą su tam tikru naudotoju);
- Galimybė sustabdyti skenavimą skenavimo eigoje (taip pat susiejant skenavimą su tam tikru naudotoju);
- Galimybė peržiūrėti ir komentuoti (atsakymai į naudotojo komentarus) skenavimo rezultatus, jų istoriją, juos eksportuoti į XLS/PDF/HTML formatus (taip pat susiejant skenavimą su tam tikru naudotoju);
- Galimybė keisti skenavimo rezultato vertinimą, jei naudotojo pateikta informacija įrodo, kad gautas pranešimas apie pažeidžiamumą yra klaidingai-teigiamas;
- Galimybė realiu laiku stebėti ateinančius log įrašus iš sistemos komponentų (nustatant tam tikrus pranešimų tipus), taip pat dirbti su archyviniais log įrašais (peržiūrėti pagal įvairius užklausų parametrus, atlikti raktinių žodžių paiešką);
- Galimybė turėti informacinį valdymo langą (angl., Dashboard), atvaizduojantį aktualią informaciją apie sistemos ir jos naudotojų statusą (sistemos

apkrautumas, prisijungusių naudotojų skaičius, suvestinė pažeidžiamumų statistika);

- Galimybė atnaujinti (arba nustatyti automatinius atnaujinimus) pažeidžiamumų aptikimo taisykles įvairiems pažeidžiamumų paieškos moduliams.
- Administratorius taip pat turi tiesioginę prieigą prie visų AISAP komponentų naudodamas tipinę komandinės eilutės sąsają, skirtą netipiniams, gilesnio konfigūracijos detalumo reikalaujantiems darbams.
- Ryšys tarp kliento ir serverio dalies užtikrinamas per šifruotą Interneto ryšį (HTTPS protokolas).

AISAP web serverio funkcionalumas:

- Atsakingas už naudotojo sąsajos formavimą (palaikomos visos šiuo metu plačiai naudojamos naršyklės);
- Vartojo sąsajos modulinio principo užtikrinimas (papildomų modulių / funkcionalumo atsiradimas ateityje; turinio valdymas – galimybė talpinti bei redaguoti skelbimus, naujienas, įspėjimus apie pagrindinius / labiausiai aktualius pažeidžiamumus, keisti kontaktinę informaciją);
- Užklausų pateikimas ir atsakymų surinkimas iš web-servisų;
- Atlieka reikiamus kompiuterinius skaičiavimus, generuoja ataskaitas ir kitas funkcijas.

WEB servisų funkcionalumas:

- užklausų priėmimas iš WEB serverių, jų konvertavimas ir perdavimas atitinkamiems pažeidžiamumų skaneriams;
- rezultatų iš pažeidžiamumų skanerių gavimas, konvertavimas ir perdavimas WEB serveriui;
- integravimo užtikrinimas su naujais komponentais.

Integracijos su kitomis LITNET sistemomis modulis:

- Užtikrina autentifikavimo mechanizmų veikimą, integraciją su LDAP / Active Directory servisais;

- Užtikrina AISAP sistemos log įrašų išsiuntimą į centralizuotą žurnalinių įrašų saugyklą.

2. Skenavimo įrankis

Pažeidžiamumų skeneris yra suprantamas kaip kompiuterinė sistema, skirta automatiniu būdu aptikti saugumo spragas, susijusias su tikrinamos programinės įrangos versija, konfigūracija, nuotoline prieiga ir pan.

AISAP skenavimo įrankiu yra naudojamas atvirojo kodo produktas OpenVAS (Open Vulnerability Assessment System), platinamas pagal laisvosios programinės įrangos licenciją GNU GPL. (http://www.openvas.org/)

4 pav. OpenVas logo

Jis pasirinktas kaip tinkamiausias, atlikus egzistuojančių rinkoje skenerių palyginamąją analizę.

OpenVAS yra atvirojo kodo pažeidžiamumo skeneris ir jų valdymo įrankis. OpenVAS skirtas aktyviam kompiuterių tinklo mazgų saugumo problemų stebėjimui, įvertinant šių problemų mastą ir stebint jų pašalinimą.

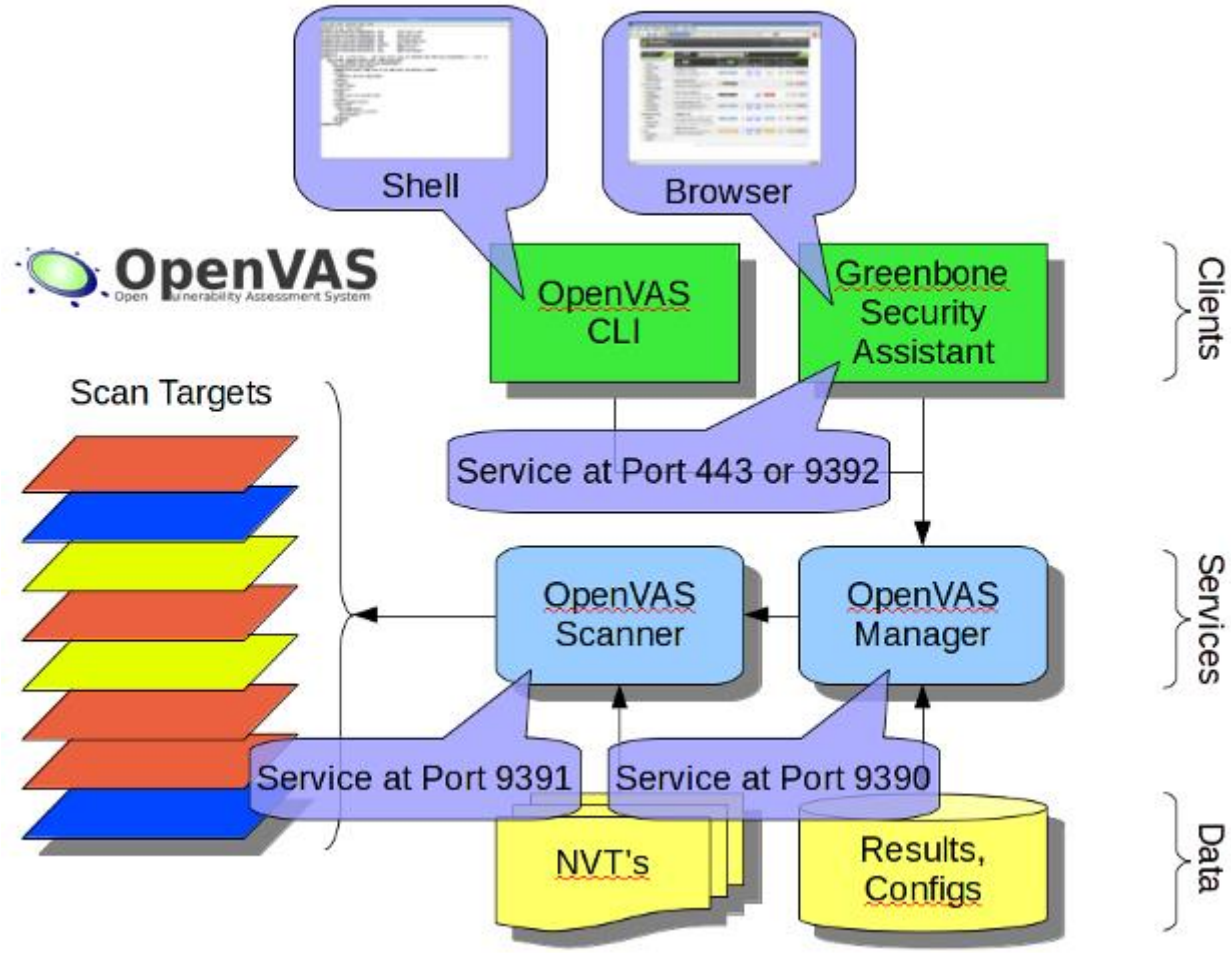
Aktyvus stebėjimas reiškia, kad OpenVAS atlieka tam tikrus veiksmus su tinklo mazgais: skenuoja atvirus prievadus, siunčia specialiai paruošta paketą imituoti puolimą ar net prisijungti (autorizuotis) prie svetainės, bando gauti prieigos prie valdymo konsolės ir atlikti komandas joje. Tada OpenVAS analizuoja surinktus duomenis ir daro išvadas apie bet kokias saugumo problemas. Šios problemos daugeliu atvejų būna susijusios su įdiegta ir nuo svetainės ar serverio sukūrimo laiko neatnaujinta programine įrangą, kurios pažeidžiamumai arba nesaugūs nustatymai žinomi ir aprašyti.

OpenVAS yra sukurtas moduliniu principu, priskiriant kiekvieną modulį tam tikram lygmeniui (5 pav.).

Kliento (paslaugos naudotojo) lygmenį sudaro OpenVAS naudotojo kevalą (Shell) formuojantis kliento (OpenVAS CLI) modulis ir peržvalgos langą (Browser) formuojantis (Greenbine Security Assistant) modulis.

Paslaugų (Services) lygmenį sudaro OpenVAS skeneris (OpenVAS Scanner) bei OpenVAS administratorius (OpenVAS Manager).

Duomenų lygmenyje yra tinklo pažeidžiamumų testų (NVT‘s) ir testavimo rezultatų bei konfigūracinių duomenų saugojimo (Results, Configs) moduliai.



5 pav. Modulinė OpenVAS architektūra **(www.openvas.org)**

4. Paslaugos naudotojai

Automatinio informacijos saugumo audito paslaugoje (https://aisa.vgtu.lt) yra dvi naudotojų grupės:

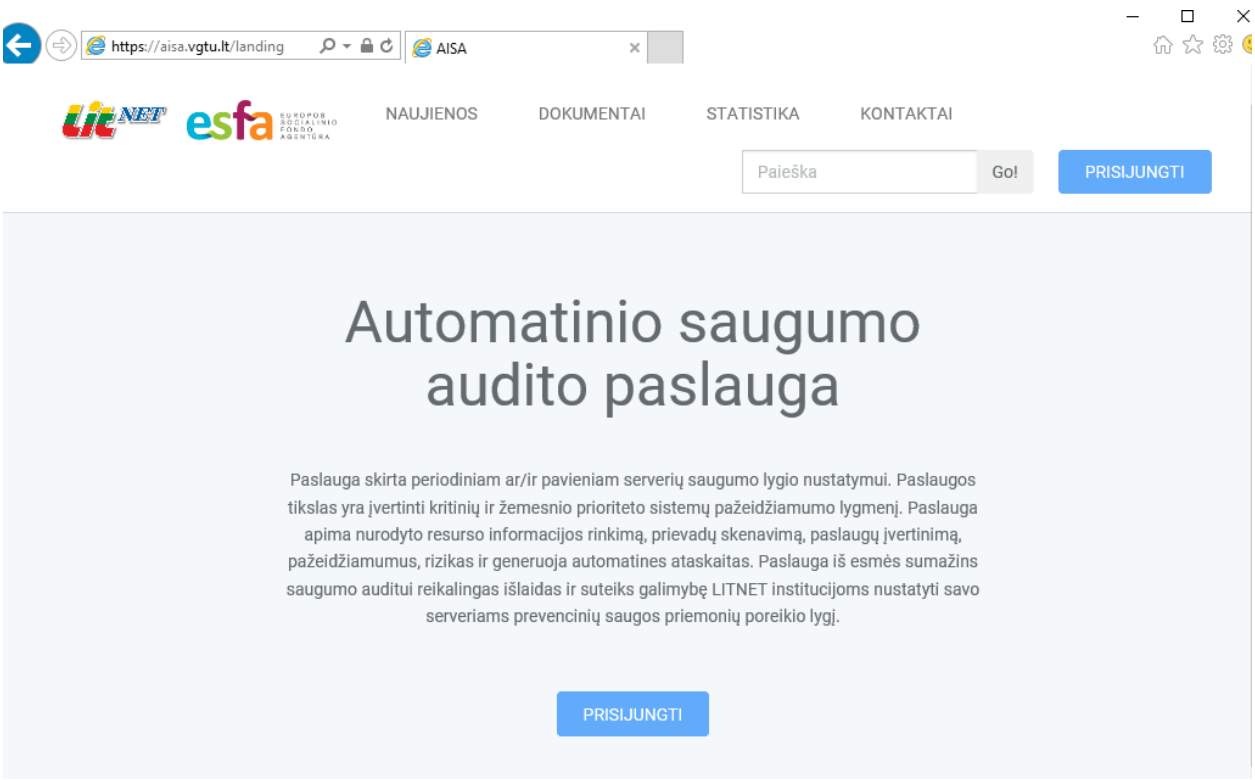
- *Naudotojai*. Ši rolė suteikiama MSI kompiuterių specialistams ar kitiems darbuotojams (mokslininkams, tyrėjams) norintiems atlikti savo naudojamų kompiuterinių resursų (serverių, interneto svetainių) saugos auditą. Naudotojai gali atlikti veiksmus, reikalingus saugos audito planavimui, vykdymui bei rezultatų valdymui savo audituojamuose serveriuose bei interneto svetainėse.
- *Administratoriai*. Ši rolė suteikiama paslaugą administruojančio ar kito Litnet techninio centro darbuotojams. Administratoriai gali atlikti saugos audito planavimo, vykdymo bei rezultatų valdymo veiksmus visame *Litnet* tinkle, taip pat atlikti paslaugos portalo bei informacinės sistemos administravimo veiksmus.

4.1 Paslaugos naudotojo web aplinka

Šiame skyriuje aprašoma naudotojo rolę turinčio naudotojo web sąsaja, per kurią prisijungęs naudotojas gali valdyti jo sukurtus sistemų testavimus bei rezultatus. Tam galima naudoti visas šiuo metu plačiai naudojamas naršykles, tokias kaip *Internet Explorer*, *Mozilla Firefox*, *Google Chrome*.

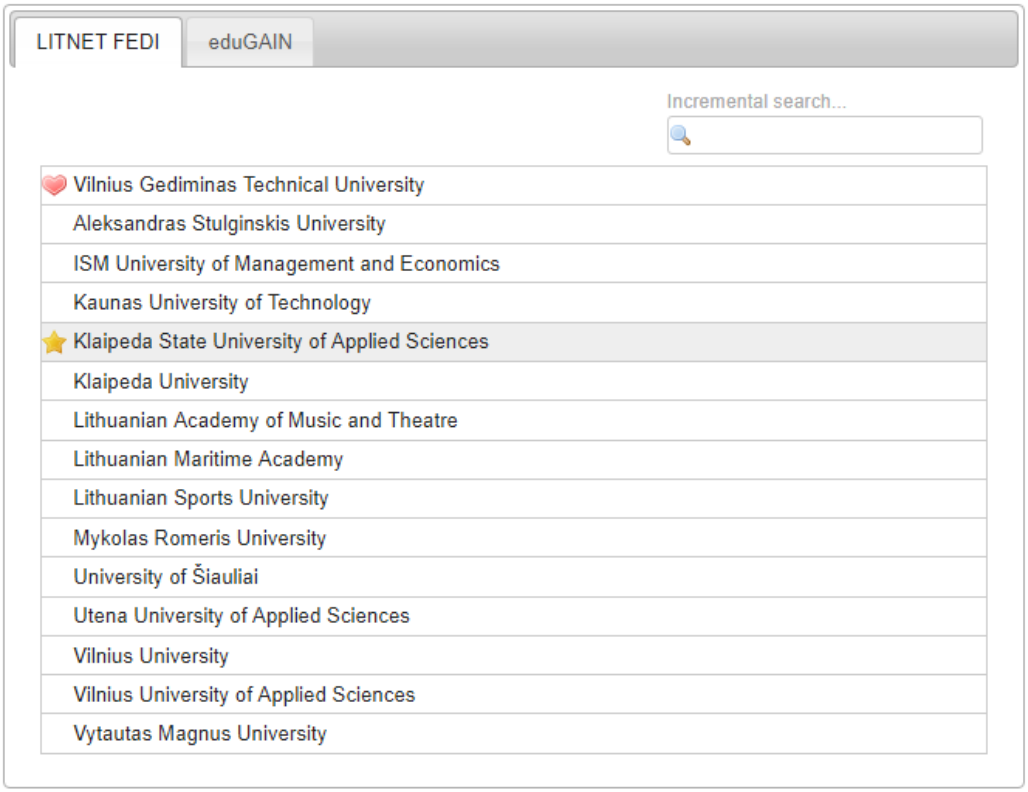
Automatinio saugos audito paslauga naudotis gali tik užsiregistravę ir gavę registracijos patvirtinimą iš paslaugos administratoriaus.

Paslauga pasiekiama adresu https://aisa.vgtu.lt arba https://www.litnet.lt/lt/paslaugos. Jos titulinis langas pateiktas 6 paveiksle.



6 pav. Titulinis paslaugos langas

Pirmą kartą jungiantis prie paslaugos norintis ja naudotis asmuo turi užsiregistruoti paslaugai per Litnet elektroninių tapatybių federaciją LITNET FEDI. Atitinkamas registracijos langas pasirodys paspaudus mygtuką ***Prisijungti*** (žr.7 pav.).

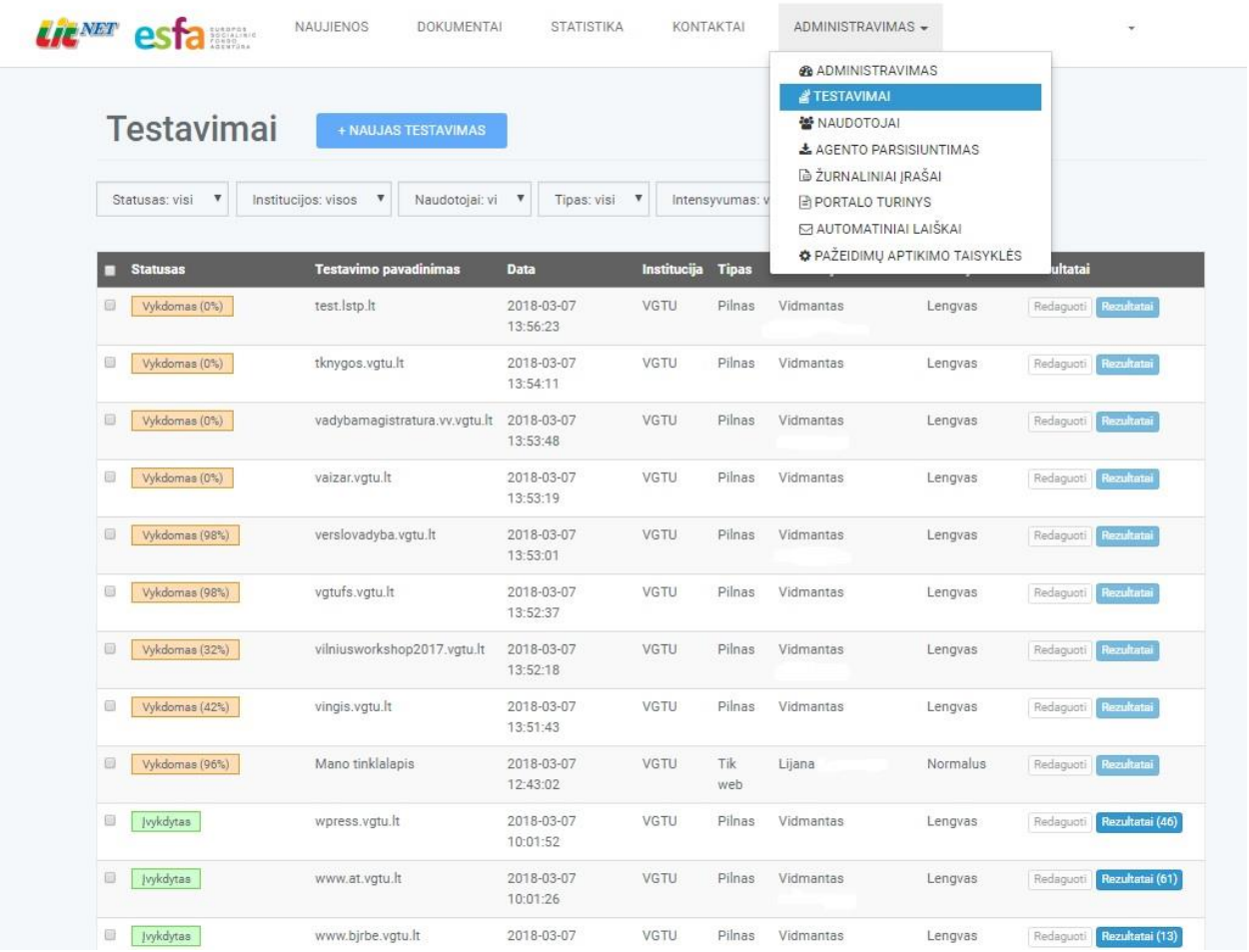


7 pav. LITNET FEDI prisijungimo langas

Po registracijos paslaugos administratorius suteikia teisę naudotis paslauga.

4.2 Paslaugos administratoriaus web aplinka

Paslaugos administratorius prie savo web aplinkos jungiasi per naršyklę adresu https://aisa.vgtu.lt. Administratoriaus aplinka analogiška naudotojo aplinkai, tik turi daugiau paslaugos administravimo įrankių, pateikiamas visų testavimų sąrašas (žr. 8 pav.)



8 pav. Paslaugos administratoriaus pagrindinis langas

Detalesni paslaugos administratoriaus veiksmai yra aprašyti skyriuje Administratoriaus funkcijos.

5. Automatinio saugos audito (testavimų) vykdymas

Automatinis saugumo auditas vykdant pažeidžiamumų testavimą naudotojas gali vykdyti pradiniame paslaugos lange pasirinkęs viršutinio meniu skyrių ***ADMINISTRAVIMAS*** ir jame punktą ***TESTAVIMAI*** (9 pav.).

Detalūs paslaugos naudotojo bei paslaugos administratoriaus veiksmai yra aprašyti atskiruose dokumentuose – Paslaugos naudotojo vadove ir Paslaugos administratoriaus vadove.