KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

KOMPIUTERINIŲ TINKLŲ KATEDRA

Vilius Palšis

TINKLO SAUGUMO TYRIMAS NAUDOJANTIS EKSPERTINE SISTEMA

Magistro baigiamasis darbas

Vadovas
lekt.dr. D. Rimkus

KAUNAS, 2013

KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

KOMPIUTERINIŲ TINKLŲ KATEDRA

Vilius Palšis

TINKLO SAUGUMO TYRIMAS NAUDOJANTIS EKSPERTINE SISTEMA

Magistro baigiamasis darbas

Recenzentas
dr. R. Kavaliūnas
2013-05-24

Vadovas
lekt.dr. D. Rimkus
2013-05-24

Atliko
IFN-1/3 gr. stud.
V. Palšis
2013-05-24

KAUNAS, 2013

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLĖLIŲ SĄRAŠAS

1. ĮVADAS

Kompiuterių tinklai tampa vis svarbesni kasdieniame gyvenime ir versle. Technologinė pažanga nuolat didina programų funkcionalumą ir bendrą kompiuterinių sistemų sudėtingumą, daugėja atakos trajektorijų. Keičiasi ne tik atakų kiekiai, bet ir pobūdis bei mastas. Kompiuterių tinklai gali būti puolami tiek nedaug nusimanančių naujokų, tiek kriminalinių grupuočių ar netgi valstybių lygmeniu. Puolantysis turi pranašumą prieš besiginančią pusę, nes iš anksto beveik neįmanoma numatyti atakos laiko, taikinio ir puolimo metodų. Daugumos pažeidžiamumų aprašus galima aptikti internete, auga įsilaužimams ar tinklo skanavimams skirtų įrankių kiekis, o jais naudotis tampa vis lengviau.

Norint apsaugoti kompiuterių tinklus, neužtenka naudoti pažangiausias technologines priemones. Būtina į informacijos apsaugą žiūrėti kaip į vientisą politikų, procedūrų ir priemonių rinkinį. Informacijos apsauga plačiuoju požiūriu ir kompiuterių tinklo apsauga nėra galutinis tikslas ar produktas, tai yra nenutrūkstamas ciklinis procesas. Turimos apsaugos priemonės turi būti nuolat tobulinamos ir peržiūrimos, svarbu įvertinti realią tinklo saugumo būklę. IT saugumo įvertinimas – tai tyrimas, kurio metu nustatomi pažeidžiamumai, įvertinamos rizikos ir su jomis susietos saugumo kontrolės priemonės. Šiam procesui įmonės neretai pasitelkia tiek vidinius, tiek išorinius auditorius, įvairias technologines priemones.

Ekspertinių sistemų panaudojimas yra vienas iš tinklo saugumo įvertinimo būdų. Ekspertinė sistema – tai programinių įrankių rinkinys, skirtas spręsti tam tikros srities problemas. Šioms sistemoms reikalingos duomenų bazės, kuriose kaupiamos žinios, o jų pagalba vėliau analizuojami ir atrenkami vartotojo pateikti duomenys. Dėl tokio veikimo pobūdžio ekspertiniai produktai paprastai būna nišiniai – skirti konkrečios apibrėžtos srities tyrimui, tikslinei auditorijai. Efektyvus ekspertinių sistemų panaudojimas tinklo saugumo įvertinimo procese sumažina saugumo poreikį, užtikrina infrastruktūros atitikimą standartams ir leidžia geriau pasiruošti išorinių organizacijų auditams.

Šiame darbe ekspertinę sistemą pritaikysime tinklų saugos problemų tyrimui ir įvertinimui. Darbo užduotys yra išanalizuoti saugumo įvertinimo praktikas, ekspertines sistemas, apžvelgti ir parinkti standartus bei skanavimo įrankius, kurie galėtų būti įtraukti į ekspertinę sistemą; sudaryti skanavimo įrankiais papildytos ekspertinės sistemos prototipą ir juo ištirti bandomojo tinklo saugumo profilį.

2. TINKLO SAUGUMO ĮVERTINIMO METODŲ ANALIZĖ

2.1. Problema

Mažo ir vidutinio dydžio kompanijos paprastai turi labai ribotus išteklius, kurių dažniausiai neužtenka visapusiškam tinklo saugumo įvertinimui ir įgyvendinimui. Tyrimai rodo, kad 79% elektroninių įsilaužimo aukų buvo atsitiktinės ir buvo pasirinktos tik dėl elementarių saugumo spragų, o dauguma atakų nebuvo techniškai sudėtingos [1].

Daugumoje kompanijų stipriai apsaugomi tik atskiri, finansiškai svarbūs tinklo mazgai (angl. *node*), tačiau nėra pilno tinklo perimetro gynybos plano arba, jei jis įgyvendintas, nėra tinkamai tikrinamas ar audituojamas. Būtina užtikrinti, kad naudojamos apsaugos priemonės būtų nuoseklios, tarp jų neliktų spragų, kurios tiesiog leistų apeiti gynybos sistemas naudojantis kitais kanalais. Tobulėjant kompiuterinėms sistemoms, tokias kompiuterinių tinklų apsaugos spragas aptikti tampa vis paprasčiau ir, kol pagrindinė gynyba nuo įsilaužimų ir informacijos nutekėjimo vis dar nukreipta į atskirus tinklų mazgus, dažnu reiškiniu tampa atakos vektorių pasikeitimas. Puolami gali būti ne tik paslaugas teikiantys serveriai, kurie paprastai turi sustiprintą apsaugą, bet ir kiti, iš pažiūros nereikšmingi mazgai. Gavus prieigą prie vienos sistemos, paprastai išnaudojamas pasitikėjimo modelis, kuris reiškia, kad, pažeidus vieną sistemą, yra įmanoma atakuoti likusias kompanijos sistemas.

Efektyvi tinklo gynyba yra kelių sluoksnių (angl. *Defence in Depth*). Tokią gynybą sudaro keli sluoksniai techninių kontrolinių priemonių: ugniasienės, įsilaužimo aptikimo ir sustabdymo sistemos, antivirusinės programos, įgaliotieji serveriai (angl. *proxy servers*), kelių lygių saugumo zonos. Dėl tokio elementų kiekio ir sudėtingumo, įmonėms finansiškai ir technologiškai sunku sukurti efektyvią tinklo apsaugos sistemą. Sukūrus tokią sistemą, ją reikia nuolatos peržiūrėti, nes įvairūs technologiniai, operacijų ar verslo pasikeitimai gali įtakoti apsaugos kontrolinių priemonių efektyvumą. Taip pat reikia atsižvelgti ir į technologinius ar reguliacinius pasikeitimus už įmonės ribų: nauji pažeidžiamumai, nauji informacijos apsaugos standartai. Neretai net ir efektyvių techninių priemonių teikiamas saugumo lygis gali būti neigiamai paveiktas saugumo politikos ar jos įgyvendino silpnumo, techninių ir valdymo procesų trūkumų.

Apsaugos priemonės turi būti planuojamos atižvelgiant į visą įmonės tinklą, reguliariai audituojamos ir papildomos, peržiūrimos iš valdymo ir procedūrinių prizmių.

2.2. Saugumo įvertinimo procesai ir praktikos

Aprašyta tinklų saugumo problema gali būti sprendžiama daugeliu kelių, šiame darbe išanalizuosime keletą pagrindinių saugumo įvertinimo metodologijų ir jomis paremtus įrankius. Neretai vidutinio dydžio įmonės apsiriboja pažeidžiamumų analize, patiki savo saugumą konkrečiam

pažeidžiamumų skanavimo įrankiui ar tiesiog pasitiki perimetro gynyba ir visai neanalizuoja vidinės infrastruktūros saugumo, pasitikėdami viena gynybos linija.

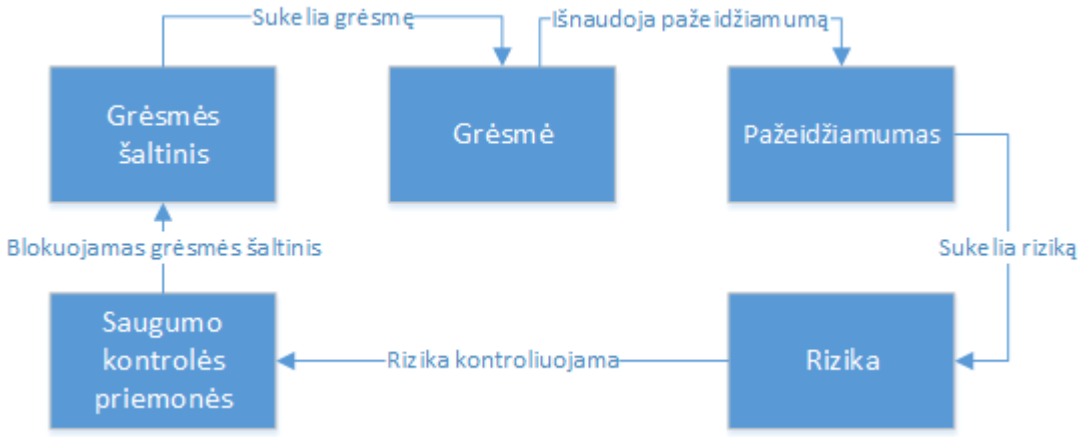
Norint efektyviai įvertinti tinklo saugumo būklę, visų pirma reikia pasirinkti efektyvią metodologiją. Įvairūs tinklo skaneriai, audito anketos ir, šiuo atveju, ekspertinės sistemos tarnauja tik kaip įrankiai, kuriais naudojantis atliekama analizė. Vienas įrankis savaime, be nuoseklaus standarto, metodologijos ir procedūrų, negali būti laikomas efektyvia saugumo įvertinimo priemone. Netinkamai parinkti skaneriai, netinkama skanavimų tvarka ar pasirinktas skanavimų dažnumas ir laikas gali stipriai įtakoti rezultatus. Gautus rezultatus, neturint papildomų techninių faktorių ar procesų konteksto, gali būti sunku interpretuoti. Visi įrankiai, standartai ir metodologijos turi būti naudojami nuosekliai, kaip bendra saugumo užtikrinimo priemonė. Vienas pagrindinių tikslų verslui lieka rizikų identifikavimas. Informacijos saugumo kontekste riziką galime suprasti kaip tikimybę, kad kažkoks veiksnys sutrukdys įmonei įvykdyti užsibrėžtus verslo tikslus. Taip gali atsitikti dėl finansinių praradimų, reputacijos netekimo, teisinių aplinkybių, verslo reguliacinių aplinkybių. Rizikoms perteikti naudojamos kokybinės (1) ir kiekybinės išraiškos (2). Kiekybinės išraiškos atveju ALE (angl. *Annual Loss Expetency*) ir SLE išreiškiami piniginiais vienetais, o ARO – tikimybe nuo 0.00 (negalimos grėsmės) iki 1.00 (garantuotai įvykstanti grėsmė) ir >1.00 (grėsmės, pasitaikančios kelis kartus per metus). Grėsmės, kurių tikimybė yra lygi nuliui, paprastai atmetamos ankstyvojo įvertinimo stadijoje.

$$\text{Rizika} = \text{Grėsmė} \times \text{Pažeidžiamumas}; \quad (1)$$

$$\text{ALE} = \text{SLE} * \text{ARO}. \quad (2)$$

Organizacijoms ne visada gali pavykti nustatyti kiekybines rizikas dėl sunkiai pamatuojamų faktorių, tokių kaip vartotojų pasitikėjimas, reputacija ir jos praradimas. Dėl to dažnai pasirenkamas kelias, kur visi lygties elementai išreiškiami įverčiais: Maža(s), Vidutinė(-is), Didelė(-is) (1).

Šiuo darbu nesiekiama išanalizuoti rizikų ar konkretaus poveikio verslui, tačiau ši sąvoka suteikia būtiną kontekstinę informaciją. Rizikas sukelia pažeidžiamumai, veikiami grėsmių. Dėl to, norint apibrėžti rizikas, reikia žinoti, kokie pažeidžiamumai egzistuoja tinkle. Viena iš saugumo įvertinimo užduočių yra surasti aktualius tinklo pažeidžiamumus ir užtikrinti, kad yra įgyvendintos būtinos priemonės šių pažeidimų kontrolei.



1 pav. Saugos sampratų tarpusavio ryšys

Šio darbo metu bus tiriamas kompiuterinių tinklų techninis domenas ir su juo susijusios procedūros, todėl tyrimas apims grėsmes, pažeidžiamumus ir jų kontrolės priemones šioje srityje. Darbe atsižvelgiama į visą CIA triadą: informacijos konfidencialumą, vientisumą ir prieinamumą.

1 lentelė Grėsmių sąrašas, paremtas NIST 800-30 dokumentu

Grėsmės šaltinis	Motyvacija	Grėsmė
Programišiai	Iššūkis Ego Maištavimas	Sistemų sugadinimas Socialinė inžinerija Įsilaužimas į sistemas Neteisėtas sistemų naudojimas
Kompiuterių nusikaltėliai	Informacijos sunaikinimas Neteisėtas informacijos atskleidimas Pelnas Neteisėtas duomenų pakeitimas	Kompiuteriniai nusikaltimai (pvz. persekiojimas e-erdvėje) Klastojimas (Pakartotino persiuntimo atakos, perėmimo atakos) Apsimetinėjimas (Kitu asmeniu arba apsimetinėjimas sistemos lygiu) Įsilaužimas į sistemas Papirkinėjimas siekiant išgauti informaciją.
Teroristai	Šantažas Naikinimas Išnaudojimas Kerštas	Kibernetinis karas Sistemų puolimas (pvz.: DDoS) Įsilaužimas į sistemas
Industriniai šnipai (Konkuruojančios kompanijos, užsienio šnipai)	Konkurencinis pranašumas Ekonominis šnipinėjimas	Sistemų pakeitimas Ekonominis išnaudojimas Informacijos vagystė Asmeninio privatumo pažeidimas Socialinė inžinerija Įsilaužimas į sistemas Neteisėtas sistemų naudojimas
Vidiniai darbuotojai (prastai apmokyti, piktavališkai nusiteikę, atleisti darbuotojai, aplaidūs darbuotojai)	Smalsumas Ego Žinios (jų trūkumas) Pelno siekimas Kerštas Netyčinės klaidos/aplaidumas	Šantažas Apribotos informacijos peržiūrėjimas Sistemų išnaudojimas ne pagal paskirtį Apgavystės ir vagystės Informacijos perėmimas Kenkėjiškas kodas Asmeninės informacijos pardavimas Sisteminės klaidos Įsilaužimas į sistemas Sistemų sabotažas Neteisėtas sistemų naudojimas

Tokios grėsmės, kaip fizinės įrangos vagystės, darbuotojo užpuolimas ar stichinės nelaimės, nėra įtrauktos į įvertinimą, nes su jomis susietas kontrolės priemones sunku įvertinti vien tik programiškai, reikalinga profesionali patalpų ir jose įrengtų sistemų vizualinė apžiūra.

Tinklo infrastruktūra yra naudojama duomenų perdavimui ir dažniausiai jų niekaip neapdoroja ir nekaupia. Nors tinklo infrastruktūra remiasi daug klientams skirtų servisų, charakteristiškai pats tinklas galutiniams klientams jų nesuteikia. Tokios domeno charakteristikos apriboja pažeidžiamumus virusams ar XSS (angl. *cross site scripting* – neleistino kodo įterpimo pažeidžiamumas) atakoms. Aktualiausi tampa pažeidžiamumai, susieti su informacijos perdavimu ir tinklo prieigos taškais.

Pažeidžiamumus galima suskirstyti į 3 bendrines kategorijas [2]:

1) Perėmimas – Duomenys gali būti perimami ar nuskaitomi perdavimo metu. Tinklai yra pažeidžiami žmogaus viduryje atakomis. Perduodami duomenys gali būti visiškai perimami įsilaužėlių, taip efektyviai sudarant ne tik duomenų konfidencialumo, bet ir visiško informacijos praradimo incidentus. Kitais atvejais piktavaliai gali pasyviai kopijuoti duomenis arba juos falsifikuoti perdavimo metu.
2) Prieinamumas – Programišiai gali sutrikdyti priėjimą prie kritinių duomenų ir taip sustabdyti kritinių paslaugų tiekimą. Tinklai yra pažeidžiami DoS ir DDoS atakoms, kurios šiuolaikinę įmonę, paremtą IT paslaugomis, gali visiškai sustabdyti, pertraukti tiek vidinę, tiek išorinę komunikaciją, sustabdyti paslaugų tiekimą klientams.
3) Prieigos taškai – Loginiai ir fiziniai taškai, iš kurių galima prisijungti prie kompiuterių tinklo, yra natūralūs pažeidžiamumų šaltiniai. Jų saugumo pralaužimas įgalina piktavalius pasinaudoti kitomis sistemos spragomis ir skverbtis gilyn į tinklo infrastruktūrą.

Praktikoje beveik neįmanoma tikėtis, kad įmonė visada naudos paskutinius programinės įrangos pataisymus dėl operacinių priežasčių: neužtenka resursų, netestuotas atnaujinimas gali neigiamai paveikti tinklo stabilumą. Neretai vykdomos ir nulinės dienos atakos, kurios apskritai neduoda laiko ištaisyti spragas. Atsižvelgiant į prieš tai pateiktas pažeidžiamumų grupes, joms ir jų keliamoms rizikoms suvaldyti naudojamos kontrolinės priemonės:

1) Perėmimo – Viena iš svarbiausių kontrolės priemonių yra informacijos perdavimas užšifruotais kanalais. Naudojami stiprūs kodavimo algoritmai, tokie kaip AES ar 3DES. Konkrečių algoritmų parinkimas priklauso nuo techninių galimybių, siunčiamos informacijos jautrumo, verslo reikalavimų. Nors fizinės apsaugos aspektas nėra įtrauktas į darbo apimtį, privalu pabrėžti, kad fizinės kontrolės priemonės atlieka svarbų vaidmenį bandant apsisaugoti nuo informacijos perėmimo.
2) Prieinamumo – Didele dalimi priklauso nuo išankstinių architektūros sprendimų. Reikia identifikuoti ir pašalinti sistemoje esančius SPOF (angl. *Single Point of Failure*) taškus. Tai

padaroma įdiegiant papildomas linijas su interneto paslaugų tiekėjais, naudojant perteklinę tinklo įrangą (angl. *redundancy*).

3) Prieigos kontrolė – Prie tam tikrų tinklo dalių prisijungti turėtų galėti tik saugumo politikoje apibrėžtos vartotojų grupės. Prieigos lizdai turėtų būti paskirstyti į atskirus VLAN, turėtų būti naudojamos prieigos lizdų kontrolės priemonės: naudojamas MAC adresų filtravimas ar/ir 802.1x autentifikavimo protokolas.

Kontrolinės priemonės skirstomos į tris grupes: administracinės, techninės ir fizinės priemonės [3]. Administracinės priemonės – organizacinės kontrolės priemonės, tokios kaip dokumentacija, procedūros, rizikų analizė, įvairūs mokymai. Techninės kontrolės priemonės – programinė ir techninė įranga, tokia kaip ugniasienės, antivirusinės programos, įsilaužimo aptikimo ir prevencijos sistemos. Fizinės kontrolės priemonės – užraktai, kodinės spynos ir pan. Funkciškai visos šios priemonės skyla į dar šešias grupes:

- Apsaugančios (angl. *Preventetive*) – skirtos išvengti incidento.
- Aptinkančios (angl. *Detective*) – skirtos aptikti jau įvykusius incidentus.
- Pataisančios (angl. *Corrective*) – skirtos sutaisyti sistemą ar jos komponentus po incidento.
- Atgrasančios (angl. *Deterrent*) – skirtos atbaidyti nuo bandymų pulti sistemą.
- Atstatančios (angl. *Recovery*) – skirtos atstatyti sistemos darbą po incidento.
- Kompensuojančios (angl. *Compensating*) – skirtos pakeisti pagrindines kontrolės priemones; alternatyvos, kur tiesioginės kontrolės priemonės neįmanomos.

Kadangi praktiškai neįmanoma sustabdyti visų incidentų prieš jiems atsitinkant, visos priemonės turėtų sudaryti vieningą visumą, negalima apsiriboti tik viena funkcine priemonių klase.

2.3. Saugumo standartai

Šiuo metu egzistuoja bent keletas didelių dedikuotų saugumo standartų grupių, tokių kaip ISO 27000 šeima ir NIST standartai, taip pat geriausių praktikų rinkiniai, tokie kaip ISF - The Standard of Good Practice for Information Security, dar daugiau standartų nėra oficialiai vadinami saugumo standartais, tačiau neretai juose nurodytos IT ar organizacinės praktikos yra siejamos su informacijos saugumu (ITIL, TOGAF, COBIT). Saugumo standartai, dėl resursų stokos, darbų prioritizavimo ar valdybos abejingumo problemai, dažnai nepilnai/netiksliai pritaikomi arba išvis nepritaikomi vidutinėse ar mažose įmonėse. Tiek ISO 27002, tiek NIST 800-53 kontrolės priemonėms skirti standartai jas perteikia pakankamai aukštu ir abstrakčiu lygiu, kurį neretai, ypač smulkioms ir vidutinėms įmonėms, sunku perteikti žemesnio lygio praktinėmis priemonėmis. Pateikiame keletą dažniausiai sutinkamų standartų ir praktikų rinkinių, kurie turi didelę svarbą industrijoje:

ISO/IEC 27000 standartų rinkinys – ISO yra didžiausia tarptautinė standartizavimo organizacija. ISO 27000 standartų šeima susideda iš keliolikos saugumo standartų, iš kurių darbo kontekste svarbu paminėti:

- ISO 27001 yra informacijos apsaugos valdymo sistemos standartas (ISMS). Jis nurodo ISMS reikalavimus, įgyvendinimą, priežiūrą ir tobulinimą. Standartas padengia visų tipų ir dydžių organizacijas.
- ISO 27002 aprašo geriausias informacijos apsaugos valdymo praktikas, apibrėžia kontrolės priemones, kuriomis užtikrinamas sistemų saugumas.
- ISO 27033 yra saugumo standartas, skirtas tinklams. Jis fokusuojasi į tinklų valdymą ir eksploatavimą iš informacijos apsaugos perspektyvos. Standartas detaliau apibūdina ISO 27002 pateiktas su tinklais susietas saugumo kontrolės priemones, nurodo jų įgyvendinimo gaires.
- ISO 27005 standartizuoja informacijos saugos rizikų valdymą. Dokumente aprašomas rizikų analizės procesas, tačiau konkretūs būdai, kaip tai turėtų būti atlikta, nėra standarto dalis.

Daug šalių turi nacionalinius šių standartų atitikmenis, modifikuotus, kad geriausiai atitiktų toje šalyje iškeltus reikalavimus.

NIST standartai - National Institute of Technology (NIST) yra išleidę gausų rinkinį IT saugos standartų. Šio darbo kontekste bene svarbiausias standartas yra NIST 800-53, apibrėžiantis IT saugos kontrolės priemones. Šios priemonės yra sudėtos į vieną standartą, siekiant suvienodinti JAV institucijų saugumo standartus, apibrėžti minimalius reikalavimus.

NIST 800-30 yra NIST atitikmuo rizikos valdymo standartams, tokiems kaip ISO 27005 ar OCTAVE.

SANS CSIS: 20 Critical Security Controls (dar žinomas kaip Consensus Audit Guidelines) – privačių kompanijų ir JAV valstybinių organizacijų konsorciumo sukurtas standartas. Kuriant šį standartą siekta identifikuoti 20 aktualiausių kontrolės priemonių, kurias įgyvendinus būtų užkirstas kelias daugumos pažeidžiamumų išnaudojimui. Kuriant standartą buvo atsižvelgta į praktinius saugumo spragų aspektus, perteikta ilgametė kompanijų patirtis, bandant apsaugoti kritinę infrastruktūrą nuo įsilaužėlių [4]. Kiekvienas iš 20 standarto punktų turi atitikmenį ISO 27002 ar/ir NIST 800-53 standartuose.

ISF The Standard of Good Practice for Information Security – ISF sukurtas geriausių praktikų rinkinys, skirtas informacinių sistemų rizikų identifikavimui ir valdymui. Praktikų rinkinys pilnai padengia IT saugumo spektrą šešiuose skyriuose: saugumo valdymas, kritinės verslo programos, kompiuterių diegimas, kompiuterių tinklai, sistemų kūrimas, galutinių vartotojų aplinka. Kiekvienas skyrius gali būti naudojamas nepriklausomai nuo kitų [5].

Kompiuterių tinklų saugumo skyrius suskirstytas dar į penkias dalis: tinklų valdymas, srauto valdymas, tinklų eksploatacija, vietinio saugumo valdymas, balso perdavimo tinklai.

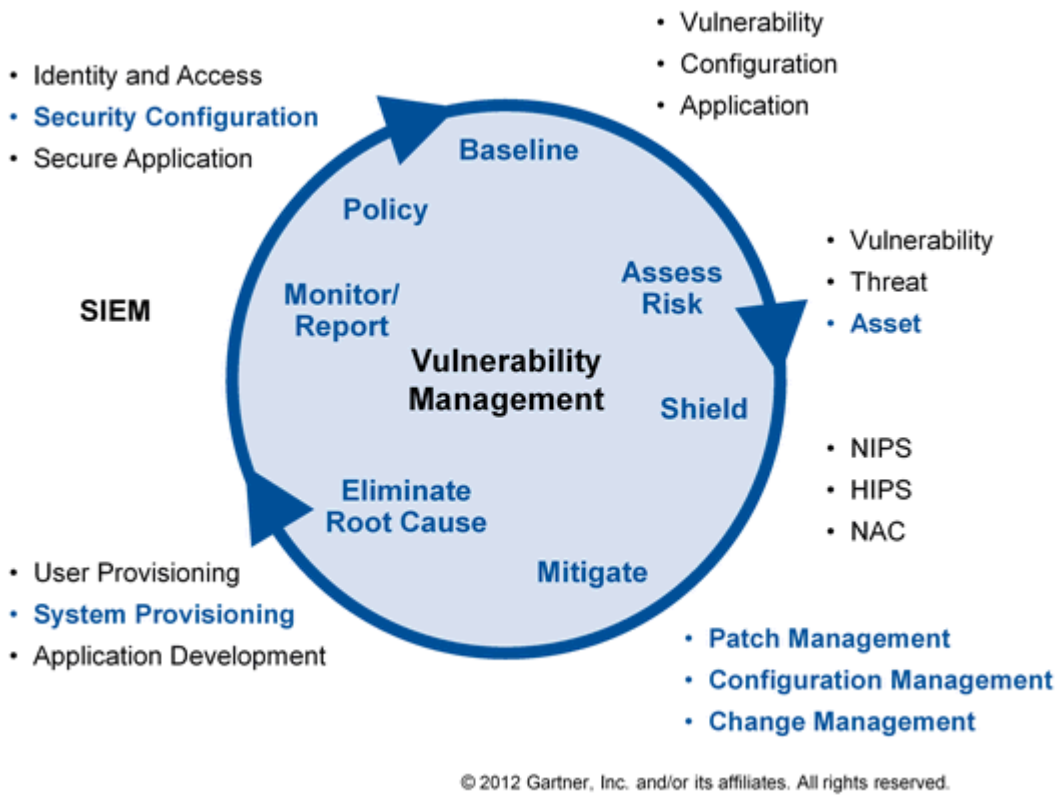
COBIT 5.0 – COBIT yra ISACA organizacijos sukurtas apjungtas plačiai naudojamų standartų ir gerų praktikų rinkinys, skirtas pagerinti įmonės valdymą. Kuriant COBIT, įtrauktas ITIL praktikų rinkinys, ISO 27000 šeimos, TOGAF ir kiti standartai.

PCI-DSS – Specifinis mokėjimo kortelių industrijos standartas, skirtas įmonėms, kurios apdoroja kortelinius duomenis. PCI reikalauja griežto šio saugumo standarto atitikimo, kas, priklausomai nuo įmonės dydžio ir svarbos, yra nuolatos audituojama. Nors PCI aktualus tik gana nedidelei rinkos daliai, poreikis atitikti šio standarto reikalavimus stipriai įtakoja pažeidžiamumų skanavimo ir valdymo sistemų rinką [6].

2.4. Realios saugumo įvertinimo sistemos

Įmonės, priklausomai nuo dydžio, finansinių ir techninių pajėgumų, specifinių infrastruktūros reikalavimų, gali pasirinkti įvairias saugumo įvertinimo strategijas. Surinkus būtinų reikalavimų sąrašą, įmonė turi nuspręsti, kiek ir kokių saugumo įvertinimo pajėgumų ji nori turėti viduje ir kiek pirkti kaip paslaugas. Tokios kompanijos kaip Qualys teikia pažeidžiamumų skanavimo ir įvertinimo paslaugas nuotoliniu būdu pagal poreikį. Taip pat gali būti užsakomos paslaugos, kai IT specialistas atvyksta atlikti saugumo įvertinimo/audito į pačią įmonę. Tokia paslauga gali būti patraukli, nes įmonei nereikia laikyti aukštos kvalifikacijos darbuotojo, pirkti saugumo programinės įrangos licenzijų ar palaikyti papildomos infrastruktūros. Reikėtų pastebėti, kad toks sprendimas turi ir neigiamų pusių: šiuolaikinėje, sparčiai kintančioje IT erdvėje, infrastruktūros, verslo procesų ar technologinis pasikeitimas už įmonės ribų, saugumo įvertinimo rezultatus gali greitai paversti pasenusiais. Dėl šios priežasties, saugumo paslaugos turi būti perkamos pastoviai, kas ne vienai mažesnius finansinius išteklius turinčiai įmonei gali būti nepriimtina. Kaip papildomas faktorius gali būti įmonės apsisprendimas išlaikyti saugumo žinias įmonės viduje, taip sumažinant priklausomumą nuo 3-iųjų šalių.

Egzistuoja labai įvairūs saugumo priemonių integravimo lygiai. Nuo sprendimų, kurie apima gana siaurą saugumo sritį, iki daugialypių produktų, kurie padengia platų saugumo spektrą. Siaurąja prasme, spragų skanavimo įrankis atranda ir informuoja vartotoją apie galimas sistemos spragas. Tačiau vartotojas susiduria su kontekstinės informacijos trūkumu, nes spraga, pati savaime, nenusako galimo poveikio infrastruktūrai. Reikia naudoti papildomas priemones, kad būtų galima įvertinti grėsmes, kontrolines priemones, riziką. Dėl šios priežasties pažeidžiamumų skanerių funkcionalumas išsiplėtė, pridėtos tokios funkcijos kaip pažeidžiamumų prioritizavimas, kontrolės priemonių įvertinimas, rekomendacijų pateikimas ir integravimas su pataisymų valdymo įrankiais.



2 pav. Pažeidžiamumų valdymo ciklas

Pažeidžiamumų valdymo ciklas (2 pav.):

- Politikos ir procesų sudarymas – apibūdina kas ir kaip tūrėtų būti konfigūruojama, vartotojų vaidmenis ir prieigos teises.
- Esamos saugumo būklės įvertinimas – siekiama išsiaiškinti egzistuojančius pažeidžiamumus ir įmonės infrastruktūros atitikimą politikai.
- Prioritizacija – priklausomai nuo pažeidžiamumų ir grėsmių, sudaromas veiksmų planas, įvertinamos rizikos.
- Apsaugojimas – diegiamos saugumo kontrolės priemonės: antivirusinės programos, papildomos ugniasienių taisyklės.
- Pataisymai – užtaisomos sistemų spragos, randamos ir eliminuojamos jų priežastys, sumažinama spragų keliama grėsmė.
- Palaikymas - sistemos palaikomos ir stebimos, valdomi jų pakeitimai.

2.4.1. Įrankiai, naudojami IT saugumo įvertinimui

Mažos ir vidutinės kompanijos pažeidžiamumų valdymui dažnai naudoja bent keletą įrankių, kurie paprastai yra mažai integruoti, jų rezultatus sunku susieti ar palyginti tarpusavyje dėl skirtingų formatų. Pažeidžiamumų aptikimui naudojami tokie įrankiai kaip prievadų skaneris NMAP. Srauto stebėjimui, analizei ar įsilaužimų aptikimui – Wireshark įrankis. Gilesnei spragų analizei prieinami tokie skanavimo įrankiai kaip Nessus. Kontrolės priemonėms ar rizikoms įvertinti naudojami

klausimynai: nuo visiškai paprastų, pildomų ranka, iki dalinai automatizuotų, tokių kaip JAV Federalinės valdžios platinamas CSET.

2.4.2. Pažeidžiamumų skanavimo įrankiai

Šie įrankiai neretai sudaro pažeidžiamumų valdymo proceso pagrindą, tačiau patys savaime nėra pilnas saugumo įvertinimo sprendimas. Surinkti duomenys įvertinami kitų įrankių ar klausimynų pagalba, neretai nedidelės įmonės į procesą turi įtraukti ir išorinius ekspertus.

Skanavimus galima suskirstyti į vidinį ir išorinį. Vidinis turi didesnes galimybes aptikti saugumo spragas, nes nėra įtakojamas perimetro gynybos priemonių. Išorinis parodo realų vaizdą, kurį gali išvysti programišius, rengdamasis atakuoti įmonės tinklą. Šiuo atveju rezultatai nebus tokie išsamūs, nes ugniasienė blokuos srautus, keliaujančius iš išorinio tinklo į įmonės vidinį tinklą. Skanavimą pagal tipą taip pat galima suskirstyti į autentifikuotą ir neautentifikuotą. Autentifikuotas skanavimas atliekamas, kai skanavimo sistema turi visus būtinus prisijungimo duomenis ir gali prisijungusi nuskaityti esamus duomenis. Autentifikuotas skanavimas yra daug detalesnis, tačiau gali padidinti įmonės pažeidžiamumą: skanavimo įranga neretai turi turėti ir saugoti administratoriaus lygio prisijungimo duomenis. Konkrečiu testiniu atveju, skaneriai turi turėti Cisco Enable (angl. *įgalinimo*) lygio slaptažodį, be jo skeneris negali įvykdyti tokių Cisco komandinės eilutės komandų kaip „*show run*“ ar „*show tech-support*“, kurios yra pagrindinės Cisco IOS naudojamos diagnostinės komandos. Skanavimus taip pat galima suskirstyti pagal sukeliamus trikdžius, į trikdančius darbą (angl. *intrusive*) ir netrikdančius. Šiuos skanavimus taip pat dar būtų galima skaidyti pagal sukeliamo triukšmo lygį, į triukšmingus ir netriukšmingus.

Tenable Nessus

Vienas dažniausiai sutinkamų pažeidžiamumų skanavimo įrankių. Jis naudoja bendrus pažeidžiamumų indikatorius, tokius kaip CVE. Nessus išsiskiria iš kitų įrankių, nes naudoja pažeidžiamumų testus, aprašytus Nessus Attack Scripting Language (NASL). Tai Nessus įrankiui sukurta kalba, kuria aprašyti pažeidžiamumų testai išbandomi ant testuojamo mazgo. Toks įrankio panaudojimas gali sukelti nenumatytų efektų testuojamoje sistemoje. Alternatyvūs įrankiai dažniausiai aptinka pažeidžiamumus naudodamiesi požymių aprašais, tokiais kaip sistemos versija ar pataisymų versija, tačiau nesiima pilno pažeidimų testavimo. Nessus diegiamas į centrinį serverį, iš kurio skanuojama tinklo infrastruktūra.

OpenVAS

OpenVAS sukurta kaip atviro kodo Nessus atšaka. Tai karkasas, susidedantis iš kelių įrankių, kurie įgalina papildomą funkcionalumą ir išplečiamumą. Pajungus papildomus pažeidžiamumų analizės įrankius, OpenVAS galima paversti iš pažeidžiamumų skanavimo sprendimo į daug platesnį

pažeidžiamumų valdymo įrankį. Siekiant aptikti sistemų spragas, OpenVAS naudojasi pažeidžiamumo testais. Darbo rašymo metu dauguma testų buvo orientuoti į galutinius mazgus: serverius, darbines stotis.

jOVAL

jOVAL yra atviro kodo OVAL kalbos įgyvendinimas, naudojantis Java. Tai pažeidžiamumų skanavimo įrankis, galintis interpretuoti daugumą OVAL objektų tipų, tačiau prieinamas tik kaip komandinės eilutės įrankis, neturinis grafinės vartotojo aplinkos ar papildomo daugumai komercinių įrankių būdingo funkcionalumo. Programa gali skanuoti tiek vietinius, tiek nutolusius tinklo mazgus ir, pasinaudojant OVAL pažeidžiamumų dokumentais, interpretuoti skanavimo duomenis. jOVAL taip pat gali būti integruotas į kitas programas kaip OVAL interpretatorius.

2.4.3. Kontrolinių priemonių įvertinimas

Surinkus pažeidžiamumų informaciją, reikia juos prioritizuoti ir įvertinti galimą riziką infrastruktūrai. Jei įmanoma, ir kai tik įmanoma, pažeidžiamumai turėtų būti užtaisyti, tačiau tai ne visada yra įmanoma. Verslo atstovai gali būti nelinkę stabdyti produkcinės sistemos, aptarnaujančios įmonės klientus, kad būtų įdiegti pataisymai dėl nereikšmingų pažeidimų ar tokių pažeidimų, kurių reikšmės tinklui negalima nustatyti. Dėl to svarbu atižvelgti į tai, kokios kontrolės priemonės egzistuoja tinkle, ar jos gali efektyviai sumažinti pažeidžiamumų grėsmę. Informacijos apsaugos kontrolės priemonės turi būti įvertintos net ir neturint informacijos apie konkrečius pažeidimus. Tai ypač aktualu kalbant apie nulinės dienos atakas, kurios gali būti įvykdytos be jokio perspėjimo iš gamintojo, pažeidžiamumų skaneriai neturės informacijos apie tokio tipo pažeidžiamus. Tokias atakas gali sustabdyti tinkamai įgyvendintos kontrolės priemonės, tokios kaip stiprios ugniasienių taisyklės, stiprūs slaptažodžiai ar jautrių duomenų kriptavimas.

Information Protection Assessment Kit (IPAK)

Information Protection Assessment Kit (IPAK) – tai Computer Security Institute (CSI) saugumo įvertinimo produktas. Šis įrankis sukurtas naudojantis Microsoft Excel, todėl vartotojo sąsajos atžvilgiu yra intuityvus daugumai vartotojų. Įrankis savo struktūra pakankamai paprastas: klausimai suskirstyti į kelis lapus pagal jų specifiką, atsakymai vertinami nuo 1 iki 10 balų. Klausimai remiasi kontrolės priemonių patikra pagal ISO 27002 dokumentą. Galutinis rezultatas gaunamas tiesiog sudedant klausimų taškus pagal kategorijas ir galiausiai sudedant atskirų kategorijų rezultatus.

Cyber Security Self Evaluation Tool (CSET)

Cyber Security Self Evaluation Tool (CSET) yra JAV vyriausybinės organizacijos Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

sukurtas įrankis, skirtas kompanijų saugumo lygiui įvertinti. Įvertinimas, naudojantis CSET, susideda iš kelių fazių:

1) Pasirenkamas standartas/-ai, pagal kuriuos bus vertinamas įmonės saugumas. Naudojami standartai: NIST 800-53, NIST 800-82, įvairūs industrijos šakoms būdingi standartai.
2) Parenkamas saugumo reikalavimų lygis (angl. *Security Assurance Level (SAL)*). Saugumo lygį nustatyti padeda trumpa kokybinė rizikos analizė. Vartotojas nurodo, kas gali atsitikti kritiškai pažeidus sistemas (darbuotojų sužeidimai, galimos mirtys, finansiniai nuostoliai, teisiniai/reguliaciniai pažeidimai ir pan.). Gautas saugumo reikalavimų lygis gali būti vertinamas nuo žemo iki labai aukšto, nuo to priklauso, kaip griežtai vertinama varotojo infrastruktūra, įvertinimo metu užduodamų klausimų skaičius.
3) Vartotojas į sistemą įkelia ar joje nubraižo loginę infrastruktūros, mūsų atveju – tinklo, diagramą, pagal kurią programa dinamiškai sugeneruoja atitinkamus bendrinius klausimus. Šie klausimai nepriklauso nuo konkretaus standarto, bet atspindi bendras geras saugumo praktikas.
4) Vartotojas atsako į klausimus pagal pasirinktą standartą bei į klausimus, sugeneruotus iš nubraižytos diagramos.
5) Remiantis pirmais keturiais punktais, pateikiama vartotojo infrastruktūros saugumo analizė.

CSET turi gerai išvystytą grafinę vartotojo sąsają, plačią dokumentaciją, dėl to programa naudotis gali ne tik saugumo industrijos profesionalai. CSET išsiskiria galimybe apdoroti tinklo loginę diagramą. Tinklo padėties analizė, nesiremiant vien tik standartiniais klausimais, gali padėti išvengti saugumo spragų, suteikti papildomos informacijos. Tačiau reiktų pastebėti, kad tokia analizė remiasi vartotojo infrastruktūros supratimu, administratoriaus perteikta schema gali neatitikti realios padėties, būti neobjektyvi.

2.4.4. Pažeidžiamumų valdymo įrankiai

Minėtieji įrankiai dažnai negali atlikti pilno saugumo įvertinimo arba jį išskaido į keletą ar net keliolika žingsnių, naudojant skirtingus įrankius, ko pasekoje, tokie procesai ne vienoje kompanijoje yra apleidžiami dėl resursų stygiaus. Siekiant atlikti pilną pažeidžiamumų įvertinimą ir palyginimą su įmonės įdiegtomis kontrolinėmis priemonėms, naudojamos pažeidžiamumų valdymo sistemos. Tai sistemos, kurios savo funkcionalumu padengia platesnį saugumo reikalavimų spektrą nei pažeidžiamumų skanavimo sistemos, dažnai gali pakeisti keletą kitų įrankių atliekant tą pačią saugumo įvertinimo užduotį. Dominuojantys išvystyti produktai yra skirti didelėms įmonėms, korporacijoms. Dažnai finansiškai arba dėl įgyvendinimo ar operavimo sudėtingumo neprieinamos mažesnėms įmonėms. Šią taisyklę kiek pakeičia faktas, kad saugumo sprendimų kompanijos pradėjo siūlyti pažeidžiamumų valdymą kaip paslaugą (angl. *Software as a Service* arba *SaaS*). Pateikiami keletas pažeidžiamumų valdymo produktų pavyzdžių:

QualysGuard

QualysGuard – tai plataus funkcionalumo pažeidžiamumų valdymo sistema. Programa gali atlikti tinklo mazgų aptikimą, prioritizaciją, aptikti ir įvertinti pažeidžiamumus, suskirstyti ir stebėti pažeidžiamumus pagal jų keliamą riziką. Qualys palaiko atskirą kompanijos pažeidžiamumų ir žinių duomenų bazę. QualysGuard pateikiama naudojantis SaaS sprendimu. Išorinis skanavimas pateikiamas be poreikio įmonei įsigyti papildomą programinę ar techninę įrangą. Tiesa, išorinio skanavimo dažnai neužtenka dėl to, kad įmonės saugumo priemonės, tokios kaip IPS ar ugniasienės, filtruoja didelę dalį skanavimo bandymų. Jei reikalingas vidinis skanavimas, reikia įdiegti Qualys skanavimo fizinį agentą, kuris perduoda vidinę tinklo informaciją QualysGuard sistemai.

Rapid7 NeXpose

Rapid7 NeXpose yra korporacijos lygio pažeidžiamumų valdymo produkto pavyzdys. Rapid 7 palaiko atskirą kompanijos žinių bazę, kurioje kaupia NexPose naudojamus pažeidžiamumų aprašus ir taisykles. Be standartinių pažeidžiamumų aptikimo funkcijų, NeXpose didelį dėmesį skiria skanavimo greičiui, sistemų aptikimui ir kategorizavimui, rizikų įvertinimui ir prioritizavimui. Į pažeidžiamumų valdymą žiūrima kaip į ilgalaikį procesą, sistema turi galimybes sekti pažeidžiamumus, paskirstyti pataisymo darbus, kurti progreso ataskaitas, skirtas tiek techniniam personalui, tiek vadovams. NeXpose sistema duomenų apdorojimui naudoja Rete algoritmu paremtą Jess (angl. *Java Expert System Shell*) ekspertinę sistemą [7]. Tokios sistemos panaudojimas ir jos taikomi euristiniai analizės metodai yra pateikiami kaip išskirtinė programos savybė.

2.5. Pažeidžiamumų aptikimo automatizavimas

Nauji pažeidžiamumai atsiranda be sustojimo, į programos kodą įterpti pažeidžiamumų aprašai neteko prasmės prieš daugelį metų – tokių programų neįmanoma pakankamai greitai atnaujinti. Didėjanti verslo priklausomybė nuo IT produktų, augantis jų skaičius ir įvairovė nulemia, kad niekada neužteks resursų, be uždelsimo ištirti visus pažeidžiamumus ir į juos reaguoti. Vis didesnė svarba tenka saugumo sprendimų automatizavimui. Šiuo metu pažeidžiamumų standartizavimui naudojama specialiai šiam tikslui sukurta kalba – Open Vulnerability and Assessment Language. OVAL yra tarptautinis standartas, kuriuo siekiama propaguoti atvirą ir viešai prieinamą IT saugos turinį, kuris leistų standartizuoti įrankius ir įgalintų skirtingų gamintojų programas apsikeisti informacija. OVAL aprašyti pažeidžiamumai kaupiami įvairiose viešai prieinamose saugyklose. OVAL kalba XML failų forma nurodo, kaip aprašyti sistemos duomenis tyrimui, saugumo tyrimo testus ir atsakymų pateikimo formas.

OVAL aprašai suskirstyti į keturias pagrindines klases:

- Pažeidžiamumų – Skirti ieškoti sistemos spragų, tikrinti spragų sąlygas.

- Suderinamumo –Skirti palyginti sistemos konfigūraciją su patvirtinta veikiančia konfigūracija.
- Inventoriaus – Skirti aprašytos programinės įrangos identifikavimui.
- Pataisymų – Skirti patikrinti sistemos pataisymų lygį/versiją.

OVAL aprašuose pateikiama tokia informacija:

- Metaduomenys: metaduomenys sudaryti iš tokių duomenų kaip OVAL identifikatorius, aprašo statusas, OVAL versijos, nuorodos į XML schemą ir nuorodos į saugumo šaltinius (CVE ID, pažeidimus pateikusių organizacijų nuorodos).
- Aukšto abstraktumo apibendrinimas: žmogiškąja kalba aprašyta pažeidžiamumų, pataisymų, konfigūracijos informacija.
- Detalus testas: apibūdina patikrinimo logiką, kuri naudojama sistemos konfigūracijos, versijos ir kitų parametrų patikrinimui.

OVAL kalba yra platesnio SCAP protokolo dalis. SCAP – tai saugumo funkcijų automatizavimo protokolas, kuris susideda iš kelių atskirų dalių, kurios palengvina saugumo informacijos įsisavinimą ir panaudojimą.

Kaip alternatyvą OVAL galima paminėti NASL. Tai panašios paskirties kalba, sukurta konkrečiai Nessus skeneriui.

SCAP kalbos:

Protokolas automatizavimui naudoja bent kelias kalbas:

- Open Vulnerability and Assessment Language (OVAL).
- Extensible Configuration Checklist Description Format (XCCDF) – formatas, skirtas standartizuotai ir struktūrizuotai aprašyti ir patikrinti sistemos konfigūraciją.
- Open Checklist Interactive Language (OCIL) – kalbos paskirtis: standartizuotais būdais iš vartotojų surinkti ir interpretuoti atsakymus į pateiktus klausimus. OCIL ypač tinka tirti problemas, į kurias atsakymų negalima gauti automatizuotų skanavimų pagalba. Tai šiuo metu tobulinamas standartas, kuris dar nėra pilna SCAP dalis [8].
- Su inventoriaus aprašymo standartizavimu susijusios kalbos: Asset Identification (AI) ir Asset Reporting Format (ARF).

SCAP sąrašai:

Saugumo automatizavimui ypač svarbu, kad pažeidžiamumus, platformas ir konfigūracijos elementus būtų galima identifikuoti originaliais žymekliais. Į SCAP protokolą įtraukti aprašai, atliekantys šias funkcijas:

- Common Vulnerabilities and Exposures (CVE) – bendra pažeidžiamumų numerių priskyrimo sistema.
- Common Platform Enumeration (CPE) – standartinis būdas identifikuoti techninės ar programinės įrangos tipą.

- Common Configuration Enumeration (CCE) – paplitusių konfigūracijų identifikavimo sistema.
- Common Weakness Enumeration (CWE) – silpno programinės įrangos dizaino / kodo identifikatorius.

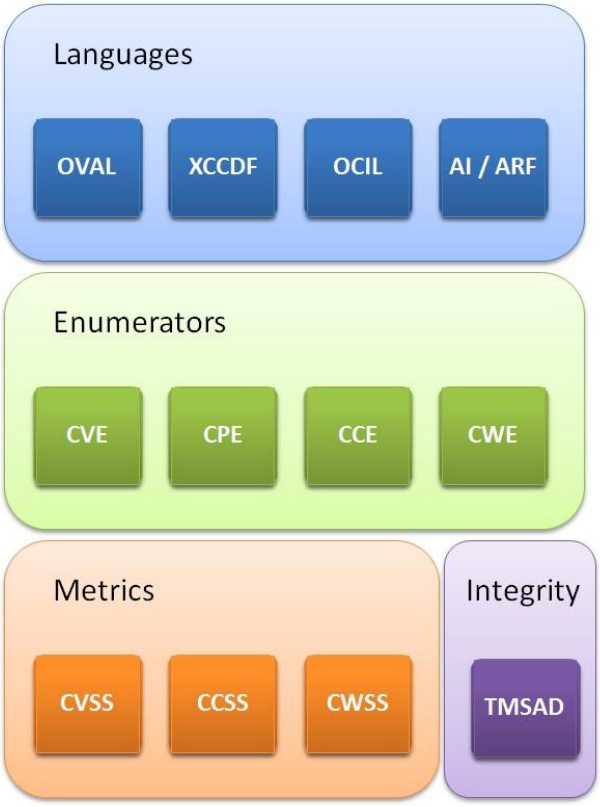
SCAP metrikos:

Svarbiausia ir labiausiai paplitusi metrika yra Common Vulnerability Scoring System (CVSS). Ši metrika padeda įvertinti pažeidžiamumo svarbą ir prioritetą. Bazinė metrikos dalis pateikiama gamintojo, tačiau vartotojai gali įtraukti papildomą komponentę, kuri parodo pažeidžiamumo svarbą konkrečiame tinkle. Be šios metrikos į standartą dar įtrauktos:

- Common Configuration Scoring System (CCSS);
- Common Weakness Scoring System (CWSS).

SCAP vientisumas:

Trust Model for Security Automation Data (TMSAD) yra modelis, skirtas palaikyti saugumo duomenų autentifikaciją, vientisumą ir atsekamumą.



3 pav. SCAP protokolo sudėtis [9]

2.6. Ekspertinės sistemos pažeidžiamumo valdyme

Pažeidžiamumų valdymui, kaip pilnas sprendimas ar, dažnesniu atveju, kaip viena iš sprendimo/architektūros detalių, gali būti naudojama ekspertinė sistema. Tokia sistema gali padėti įvertinti surinktą pažeidžiamumų informaciją. Ekspertinės sistemos, priklausomai nuo konfigūracijos ir keliamų tikslų, geba palyginti informaciją su turimų pažeidžiamumų ar atakų šablonais,

kompleksinės logikos pagalba aptikti pažeidžiamumu net kai sistema neturi tikslaus pažeidžiamumo aprašo. Dialoginę vartotojo sąsają naudojanti sistema geba surinkti ir įtraukti į analizę informaciją, kurios neišeina surinkti paprastais skanavimo įrankiais. Tai gali būti tinklo parametrai, kurių nebuvo įmanoma surinkti dėl naudojamų saugumo sistemų, įmonės saugumo politika ar specifinė administratoriams žinoma informacija.

Ekspertinė sistema susideda iš trijų pagrindinių dalių: žinių bazės, programinių metodų, skirtų tos bazės analizei (taisyklių variklio), ir vartotojo sąsajos. Žinių bazėje kaupiama iš ekspertų surinkta informacija, kuri vėliau, priklausomai nuo programos reikalavimų, įvedama taisyklių išraiška.

Siekiant lengviau suprasti kodą ir palengvinti jo struktūrą, taisyklės dažnai atvaizduojamos programavimo sąlyginių komandų konstrukcija IF-THEN, bet yra ir daugiau metodų.

Dalis galimų taisyklių atvaizdavimo variantų [10]:

- Predikatų logika: atvaizduoja sakinį simboliais ir funkcijomis. Praktikoje net ir labai mažos sistemos yra sunkiai išplečiamos, dėl to jų plačiau nenagrinėsime.

  A *paveikia* B

  B *paveikia* C

  C *grąžina* D

  A, B, C, D šiuo atveju yra simboliai. *Paveikia* ir *grąžina* – funkcijos.

  Produkcijos taisyklės: atvaizduojamos sekomis IF-THEN kaip sąlygos bei įvykiai ir rezultatai.

  IF *sąlyga I* AND *sąlyga II*

  THEN *įvykis I* AND *įvykis II* AND *įvykis III*
- Objektais ir semantinėmis taisyklėmis: labiausiai struktūrizuotas variantas, vaizduoja objektus ir ryšius tarp jų.
- Procedūrinės programos: dalis žinių gaunama atlikus matematinius skaičiavimus.

Vien tik žinių atvaizdavimo taisyklėmis modelio neužtenka, turi būti efektyvūs metodai žinių iškvietimui ir panaudojimui. Tam naudojamas išvadų modulis (angl. *Inference engine*), kuris atsakingas už navigaciją po žinių bazę ir pačių išvadų priėmimą. Egzistuoja du pagrindiniai metodai žinių perrinkimui:

- Tiesioginės grandinės metodas (angl. *Forward chaining*) – dar vadinamas „valdomas duomenimis“ (ang. *Data Driven*). Darbinėje atmintyje esantys duomenys yra lyginami su taisyklių IF dalimis ir taip nustatoma, kurią taisyklę paleisti. Sutapus IF daliai, įsimenama prielaida, tuomet atliekama THEN dalis. Surinkus pakankamai prielaidų, generuojama išvada.

  Prielaidos:

  IF *a* THEN *b*

  IF c THEN *e*

  Išvada

IF b AND *e* THEN *g*

- Netiesioginės grandinės metodas (angl. *Backward Chaining*) – valdomas tikslais (angl. *Goal driven*). Paieška pradedama nuo tikslo, imama THEN dalis ir ieškoma, kokios turi būti sąlygos, kad prielaida būtų teisinga [11].

  Tikrinamas f:

  IF *a* AND *g* THEN *f*

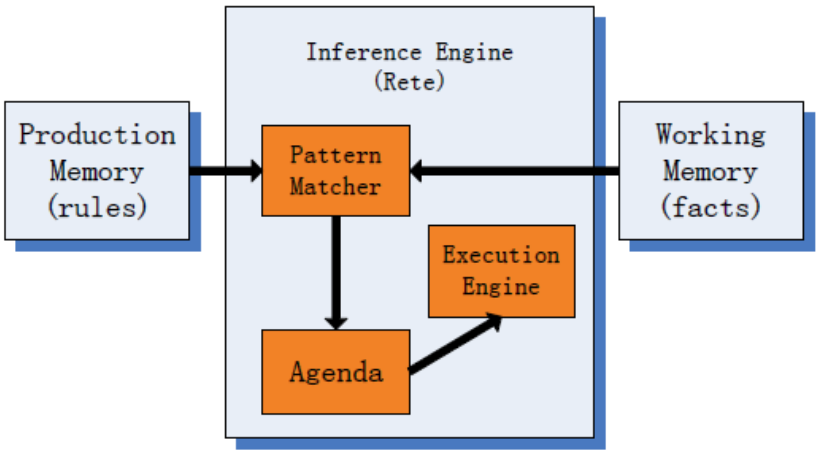
  Norint, kad f būtų tiesa, *a* ir *g* turi būti tiesa:

  IF *x* AND *y* THEN *a*

  IF *z* AND *v* THEN *g*

2.6.1. Taisyklių generatorius

Taisyklių variklio užduotis yra įvestų duomenų palyginimas su turimomis taisyklėmis. Tipinis taisyklių generatorius sudarytas iš 3 komponentų: darbinės atminties, produkcinės atminties ir parinkimo variklio. Išvadų generatorius sudaryta iš dar 3 komponentų: dėsningumo aptikimo modulio, tikslų ir vykdymo variklio. Ekspertinei sistemai vertinant faktus, visada pereinami 3 etapai: palyginimo, parinkimo ir įgyvendinimo. Rete – tai Charles L. Forgy sukurtas algoritmas, skirtas ekspertinių sistemų (taisyklėmis paremtų produkcinių sistemų) dėsningumų aptikimui. Jį naudojo beveik visi darbo metu analizuoti taisyklių varikliai ar įrankiai ekspertinių sistemų kūrimui, tokie kaip: CLIPS, Drools, Jess, Pychinko.

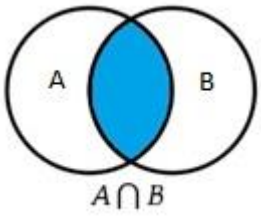


4 pav. Taisyklių generatorius [12]

2.6.2. Ekspertinių sistemų savybės

Ekspertinės sistemos gali išspręsti uždavinius, tiksliai atitinkančius jų žinių domeną. Kai kurios pažengusios sistemos gali vadovautis sudėtingomis loginėmis faktų ir sąlygų grandinėmis, kad prieitų labiausiai tikėtiną sprendimą, net jei neturi konkrečių žinių, atitinkančių sprendžiamą

problemą. Tačiau bendruoju atveju net tokios sistemos yra priklausomos nuo turimų taisyklių ir negali išspręsti visiškai su turimomis žiniomis nesusietos problemos.



5 pav. Ekspertinės sistemos žinių domeno **A** ir sprendžiamų problemų **B** ryšys

Tokia sistema nepakeistų ugniasienių ar atakų aptikimo įrankių, tačiau juos papildytų, sumažindamos poreikį samdytis konsultantus bei nuolat atlikinėti tinklo saugumo auditą.

Pagrindiniai ekspertinių sistemų privalumai [13]:

- Galimas kaštų sumažinimas – galimai sumažėja poreikis samdyti informacijos saugos konsultantus. Nors pagrindinai šaltiniai tai pateikia kaip ekspertinių sistemų privalumą, jo negalima vertinti vienareikšmiškai, kiekvienu konkrečiu atveju turi būti atliekama ROI (angl. Return On Investment – investicijos grąža) studija;
- Greitaveika – išvados generuojamos sparčiau nei tai dažniausiai galėtų padaryti žmogus – ekspertas. Tam dažniausiai įtakos turi ne tik faktas, kad žmogui reikia laiko rasti sprendimą, bet ir faktas, kad ekspertai gali būti ne visada greitai prieinami;
- Išliekamumas – informacija nėra prarandama pasibaigus darbuotojo kontraktui;
- Prieinamumas – lengvai pasiekiamos ir potencialiai prieinamos daugeliui kompanijų;
- Pastovumas – informacija nėra paveikiama tradicinių žmogiškųjų faktorių, tokių kaip emocijos ar nuovargis, yra nešališka.

Ekspertinių sistemų silpnoji vieta – žinių surinkimas. Nėra universalių metodų, kaip į sistemą įvesti ekspertų informaciją. Verčiant žinias į taisykles rankiniu būdu, išauga klaidų tikimybės. Sistemų silpnosios vietos neretai kyla ir iš pasirinktos analizavimo logikos. Norint išspręsti šias problemas, reikia samdyti žmones ne tik programos sukūrimui, bet ir palaikymui. Todėl ilgainiui programos palaikymo kaštai gali viršyti jos kūrimo kaštus [14].

2.6.3. Ekspertinių sistemų pritaikymas įvertinant tinklo saugumą

Ekspertinės sistemos naudojamos kaip įsilaužimų aptikimo ir pažeidžiamumų valdymo sistemų dalis. Tokios žiniomis paremtos sistemos laikomos gana tiksliomis, tačiau reikalauja nuolatinio žinių bazės atnaujinimo. Vienas didžiausių privalumų, šiuo atveju, yra, kad tokios sistemos sumažina klaidingų aliarmų kiekius bei padidina šansus apsisaugoti nuo nulinės dienos atakų. Nors dauguma komercinių tinklo saugos skenerių neskelbia tikslaus savo veikimo principo, dalis jų artimi ekspertinėms sistemoms dėl pažeidžiamumų antspaudams aptikti naudojamų taisyklių generatorių.

Darbo metu sieksime sukurti tinklo saugumo sistemos prototipą, orientuotą į vidutinio dydžio įmones. Tokio tipo sistema turėtų atlikti centrinį vaidmenį saugumo įvertinime ir apjungti dabar rinkoje egzistuojančius įrankius, siekiant pateikti sistemingą tinklo infrastruktūros saugumo informaciją.

Nišos įmonės veikloje, į kurias orientuota siūloma tinklo apsaugos sistema:

- Periodiniam tinkle saugumo įvertinimui atlikti;
- Pradinei saugumo analizei atlikti besiruošiant išoriniam auditui;
- Saugumo sprendimų parama.

Sistema apjungtų ir papildytų paprastesnius metodus ir įrankius, tokius kaip periodiniai rankiniai prievadų skanavimai, naudojantis prievadų skanavimo programomis, ar administratoriaus atliekama prietaisų konfigūracijos patikra, siekiant patikrinti sistemos pataisymų versijas.

Tokia sistema galėtų būti alternatyva dabar plintančioms SaaS tipo pažeidžiamumų valdymo paslaugoms. Tokio tipo paslaugos gali efektyviai atlikti išorinio perimetro skanavimą, tačiau dažniausiai negali realiai įvertinti saugumo spragų, egzistuojančių vidinėje tinklo infrastruktūroje. Tokie skanavimai negali įvertinti kelių sluoksnių apsaugos priemonių ar jų efektyvumo, taip realiai susilpninant šios strategijos pritaikymą.

2.7. Analizės išvados ir darbo tikslas

Šiuo metu egzistuoja labai didelis kiekis įvairių sprendimų, skirtų pažeidžiamumų, kontrolės priemonių ar saugumo platesne prasme įvertinumui, tačiau jie ne visada sėkmingai įgyvendinami. Tai nulemia tiek techninės, tiek organizacinės priežastys. Vyraujančios techninės priemonės yra labai įvairios apimties, nuo konkretaus sistemos parametro iki sudėtingesnių priemonių, kurios identifikuoja konkrečius pažeidžiamus. Didelės korporacijos naudoja sudėtingus ir brangius pažeidžiamumų valdymo įrankius, kurie gali ne tik aptikti pažeidžiamus, bet įvertinti šių pažeidžiamumų kompanijos tinklui sukeliamą riziką. Tai, kartu su procesų spragomis ir saugumo standartizavimo trūkumais, nulemia statistinę tendenciją, pagal kurią įsilaužimų taikiniais dažnai tampa vidutinės ar mažos įmonės. Įsilaužimai dažnai būna nesudėtingi ir lengvai sustabdomi. Dėl šių priežasčių egzistuoja niša nedidelius resursus turinčių įmonių segmente, kurios negali įsigyti ar įdiegti sudėtingų ir brangiai kainuojančių sprendimų. Įrankių apžvalga parodo didelį pažeidžiamumų aptikimo sistemų kūrėjų dėmesį galutiniams mazgams. Mažiau dėmesio skiriama pačiai duomenis perduodančiai tinklo infrastruktūrai. Tačiau reikia pastebėti, kad tinkamai apsaugotas tinklas gali neretai padėti palengvinti galutinių mazgų saugumo problemą.

Pažeidžiamumų įvertinime ryškėja tendencija standartizuoti ir automatizuoti procesus. Vietoje uždarų komercinių standartų, sąlygojančių įrankių sudėtingumą, ryškėja vieši standartai, tokie kaip SCAP protokolas ar OVAL pažeidžiamumų įvertinimo kalba. Naudojantis šiais standartais,

potencialiai galima integruoti skanavimo priemones su kitais sprendimais, tokiais kaip ekspertinės sistemos, kurios, remiantis saugumo standartais ir praktikų rinkiniais, gali daryti išvadas iš surinktų duomenų.

Darbo tikslas:

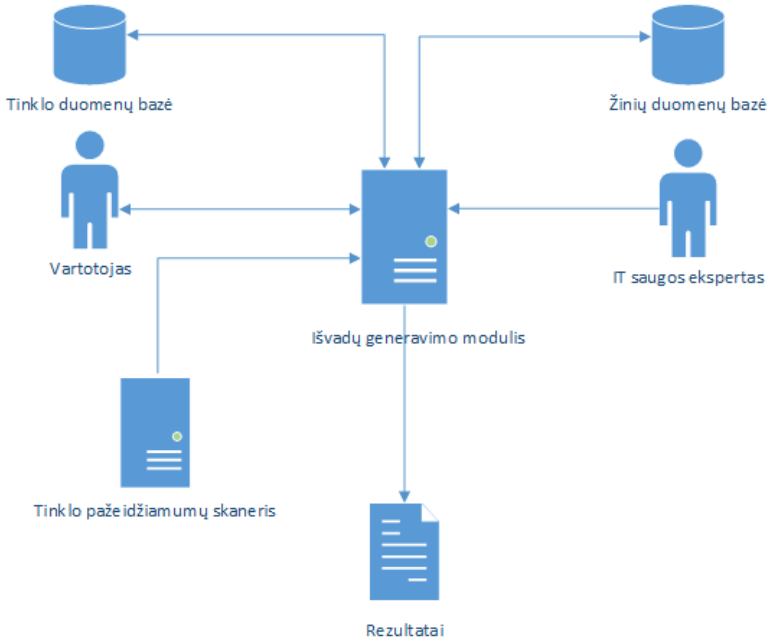
Pasiūlyti tinklo saugumo įvertinimo metodą, paremtą ekspertinėmis sistemomis bei sukurti ekspertinės sistemos prototipą, papildytą automatizuotomis priemonėmis, ir juo įvertinti tinklo saugumą.

Siekdami tikslo, atliksime šiuos uždavinius:

- Pasirinkti metodus ir sprendimą, tinklo saugumui įvertinti skirtos ekspertinės sistemos prototipo sudarymui.
- Įvertinti galimus tokio prototipo pranašumus ir trūkumus, tinklo saugumo uždavinių sprendimui.
- Įvertinti saugumo automatizavimo metodologijų pritaikymą, siekiant sumažinti klaidingų spragų skaičių ir taip supaprastinti saugumo įvertinimo procesą.
- Palyginti ir pasirinkti skanavimo metodą bei saugumo standartą surinktiems duomenims įvertinti ir padengti sritims, kur skanavimai gali būti neefektyvūs ar negalimi.

3. TINKLO SAUGUMO ĮVERTINIMO SPRENDIMAS, PAREMTAS EKSPERTINE SISTEMA

Siūlomoje sistemoje išvadų generatorius užimtų centrinį kontrolinį vaidmenį, surinktų ir analizuotų iš papildomai įdiegtų skanerių gaunamą informaciją. Dėl orientacijos į resursų stokojančias įmones, realizacija turėtų būti kaip galima labiau automatizuota, vartotojo pusėje ženklią dalį duomenų turi sudaryti automatinių ar dalinai automatinių įrankių surenkama informacija. Būtinos sąsajos tarp tinklo skenerių ir analizės modulio bei vartotojo sąsaja tinklų saugos ekspertams. Sąsaja su tinklo skeneriais turėtų būti kaip įmanoma universalesnė, tam tikslui, priklausomai nuo konkrečių įrankių galimybių, numatoma naudoti tekstinius failus, tokius kaip xml. Tai išpildytų modulinės sistemos koncepciją, neprisirišant prie vieno konkretaus komercinio formato.



6 pav. Koncepcinis skaneriu papildytos ekspertinės sistemos modelis

Minimalūs tinklo skanavimui keliami reikalavimai: aptikti TCP/UDP prievadus, MAC ir IP adresus, operacinės sistemos versiją ir tipą. Labai svarbi yra tinklo skanavimo strategija – iš kur ir kokiomis priemonėmis bus skanuojamas tinklas, kokius veiksmus turės atlikti vartotojas, kad sėkmingai surinktų duomenis. Vienas iš pagrindinių aspektų yra pasirinkimas tarp išorinio ir vidinio sistemos skanavimo. Skanuojant iš išorės, pavyktų surinkti daug mažiau informacijos, nei skanuojant iš vidaus.

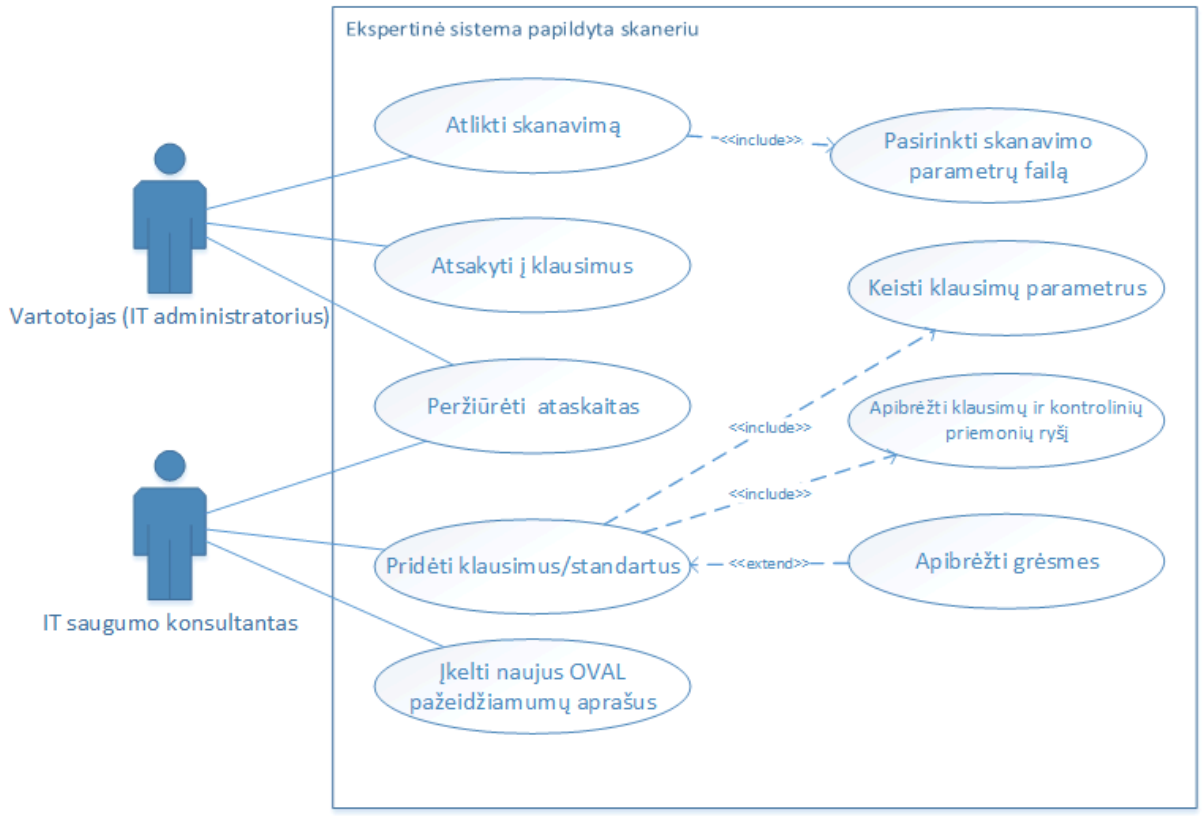
Egzistuoja abipusė priklausomybė tarp skanerio surenkamų duomenų ir žinių bazių. Bandymų metu surinktų duomenų kiekis ir kokybė gali reikalauti žinių bazės pokyčių, optimizavimo, papildomų taisyklių kūrimo. Pokyčiai žinių bazėje taip pat gali sąlygoti naujus reikalavimus surinkti papildomus duomenų tipus ar atsisakyti realiai nepanaudojamų. Visgi pagrindiniai komponentai, kuriais turėtų remtis visa sistema, yra analizės modulis ir žinių bazė.

Žinių bazė bus pildoma remiantis vienu ar keliais šaltiniais, saugumo metodologijomis, geriausių praktikų rinkiniais, tokiais kaip NIST 800-53. Vienas iš pradinių sistemos įgyvendinimo darbų turi būti žinių bazės modeliavimas, siekiant išvengti nepadengtų tinklo apsaugos klausimų ir logikos spragų. Tolimesnis žinių bazės tobulinimas ir atnaujinimas turėtų vykti nenutrūkstančiais tobulinimo ir testavimo ciklais.

Metodai, skirti žinių surinkimo automatizavimui, nėra numatyti, tačiau, siekiant sistemos išplečiamumo, turėtų būti įdiegta sąsaja, skirta ekspertinių žinių įvedimui ir pakeitimui.

Nors pasiekti konkrečią greitaveiką nėra vienas iš tikslų, sistemos žinių ir duomenų bazės turėtų būti optimizuotos – jose neturėtų būti nenaudojamų taisyklių ar objektų.

Keliamai problemai ir uždaviniams spręsti bus kuriama sistema, integruojami keletas atskirų įrankių. Sistema savo išbaigtumu ir funkcionalumu yra skirta atvaizduoti siūlomą sprendimą ir testuoti integruotos ekspertinės sistemos panaudojimo teoriją vidutinio dydžio įmonės mastu. Šiuo sistemos modeliu nesiekiama įgyvendinti papildomo, nekritinio funkcionalumo.



7 pav. Panaudojimo atvejų diagrama

2 lentelė Sistemos vartotojų galimybės

Sistemos vartotojų vaidmenys ir funkcijos	
Vartotojas (IT administratorius)	**IT saugos konsultantas**
• Atlikti tinklo skanavimą naudojantis integruotais skanavimo įrankiais. • Užpildyti saugumo įvertinimo sistemos klausimyną. Atsakyti į pagal standartą sukurtus klausimus bei papildomus klausimus, aktyvuotus atsižvelgiant į tinklo skanavimo rezultatus. • Peržiūrėti sugeneruotą saugumo įvertinimo ataskaitą.	• Sukurti naujus klausimus, atsakymus, testus. Galimybė papildyti testą naujais klausimais arba išvis pakeisti įvertinimui naudojamą saugumo standartą. • Taisyti ir atnaujinti egzistuojančius saugumo įvertinimo testus. Galimybė pakeisti klausimų aktyvavimo ar išpildymo sąlygas. Pastebėjus netikslumus arba spragas, modifikuoti visus ar bet kurį klausimo elementą. • Įkelti naujus pažeidžiamumų aprašus. • Kalibruoti skanavimo sistemą. Į skanavimo sistemas pateikti papildomus parametrus, nuo kurių priklauso skanavimo trukmė, tikslumas ir skanavimo poveikis produkciniam tinklui. • Peržiūrėti sugeneruotą saugumo įvertinimo ataskaitą.

Šios sistemos prototipo atveju, neišskiriamas vartotojas ir administratorius. Dėl tipinės mažų ar vidutinių įmonių struktūros, saugumo įvertinimo užduotys dažniausiai atitenka IT administratoriams. Norint pritaikyti sistemą platesniam įmonės darbuotojų ratui, būtų reikalingas vartotojų ir administratorių atskyrimas, norint neapkrauti vartotojų grupės papildomomis techninėmis ir administravimo detalėmis. Pagrindinai prototipo tikslai:

- Sistema turi būti išplečiama: sistemos skanavimo ir testavimo galimybės negali būti apibrėžtos statiniu kodu. Sistemą galima išplėsti naujų pažeidžiamumų aprašais, kontroliniais klausimais ar, esant reikalui, pakeisti vertinimo standartą.
- Testavimo scenarijai turi būti paslankūs: neužduodami konkrečiai sistemai nereikšmingi klausimai.
- Sistema turi turėti galimybę operuoti produkcinėje aplinkoje jos kritiškai nesutrikdydama. Priimtina laikyti, kad visi skanavimai infrastruktūrai sukelia tiesioginę ar netiesioginę grėsmę, dėl galimo atsitiktinio DoS sukėlimo ar saugumo sistemų aliarmų. Grėsmės lygis gali svyruoti nuo visiškai mažos netriukšmingų žemo intensyvumo skanavimų keliamos grėsmės iki labai aukšto, kai skanavimo metu bandoma išnaudoti sistemos spragas. Nors triukšmingumo, apkrovos ir trikdymo kriterijai nėra matuojami darbo metu, laikome, kad prototipo sudėtyje galime naudoti tik įrankius, nenaudojančius aktyvių, trikdančių spragų testavimo metodų.
- Sistema turi būti integruota: daugumą veiksmų galima atlikti iš bendros sąsajos valdymo lango. Sistemos efektyvumas nėra vertinamas resursų sąnaudos ar greitaveikos aspektais.

3 lentelė Siūlomos sistemos SWOT (angl. Strenghts, Weaknesses, Oppurtunities, Threats) matrica

Stipriosios Pusės	**Silpnosios pusės**
• Sistema sudaryta iš standartinių komponentų. Naudojami tokie standartizavimo būdai kaip OVAL, XML, CVE, CVSS. • Sistema papildo pažeidžiamumo skanavimo priemonių galimybes. Galimas pažeidžiamumų, grėsmių, poveikio ir kontrolinių priemonių įvertinimas. • Mažas klaidingų pavojų skaičius, skanerių surasti pažeidžiamumai papildomai įvertinami klausimyno forma. • Sistema iškart atmeta negalimus variantus ir taip sumažina klausimų skaičių ir krūvį vartotojui.	• Pažeidžiamumų ir kontrolinių priemonių ryšys turi būti nurodomas saugumo specialisto rankiniu būdu. • Sistema priklauso nuo žinių inžinerijos, įvestų klausimų kokybės. • Sistema, kaip ir visos ekspertinės sistemos, priklausoma nuo vartotojo pateiktų atsakymų kokybės.

3 lentelė Siūlomos sistemos SWOT (angl. Strenghts, Weaknesses, Oppurtunities, Threats) matrica (tęsinys)

Galimybės	Grėsmės
• Sistemos moduliškumas leidžia sistemą nesunkiai išplėsti naujais įrankiais. Prototipo apimtis apribota, ir jį naudoti galima tik tinklo infrastruktūros skanavimui, sistemą galima nesunkiai išplėsti į galinių mazgų apsaugos domeną.	• Sistema priklausoma nuo naudojamų skanavimo įrankių kokybės. Klaidos jų įgyvendinime gali turėti įtakos saugumo įvertinimo rezultatams. • Sparčiai besivystantys SaaS saugumo įvertinimo sprendimai, dalimi atvejų, vidutinių įmonių lygyje kokybės ir kainos santykiu gali būti pranašesni už įmonės viduje įgyvendintas saugumo sistemas.

3.1. OVAL panaudojimas

Siekiant pritaikyti sistemą mažoms ir vidutinėms įmonėms, netikslinga kurti atskirą duomenų bazę, reikalaujančią intensyvaus palaikymo, ar naudoti egzistuojančią komercinę, kas reikalautų brangių paslaugų pirkimo. Dėl šių priežasčių, sprendime panaudosime atvirą OVAL kalba aprašytų pažeidžiamumų duomenų bazę ir joje kaupiamus aprašus. Iš keleto prieinamų duomenų bazių naudosime palaikomą MITRE organizacijos [15]. Pasirinkimo priežastį nulemia organizacijos žinomumas ir patikimumas, faktas, jog duomenų bazėje yra saugomi Cisco sistemoms būdingi pažeidžiamumai. Taip pat naudosime ir pačios Cisco korporacijos pateikiamus aprašus. Dėl pažeidžiamumų aprašų standartizavimo, esant reikalui, galima pakeisti aprašų šaltinį be jokių papildomų programinės įrangos pakeitimų. Aprašai gaunami XML formatu (8 pav.) [16]. Nr. 1-11 pažymėtos eilutės suteikia paprastam vartotojui suprantama kalba pateiktą pažeidžiamumo informaciją, kuri yra būtina ekspertinės sistemos dialoginiam ryšiui su vartotoju, taip pat matomas CVE pažeidžiamumo identifikatorius. Eilutėse nr. 23-34 matome informaciją, kurią skaneriai naudoja pažeidžiamumų nustatymui: loginius operatorius, žodinį testo aprašą. Užrašome šio SSL VPN patikrinimo aprašą logine forma, įsivesdami A, B, C ir D kaip tikrinamus faktus, bei X, kaip išvadą:

$$(\boldsymbol{A} \cap \boldsymbol{B} \cap \boldsymbol{C}) \cup (\boldsymbol{A} \cap \boldsymbol{D} \cap \boldsymbol{E}) \Rightarrow \boldsymbol{X}. \quad (3)$$

Šią formą galima efektyviai perteiki ir ekspertinės sistemos taisyklėmis, grupuojant kartu kaip vieną patikrinimą, arba pateikti įvertinimą kaip dvi taisykles, taip supaprastinant užrašymo tvarką:

$$\boldsymbol{A} \cap \boldsymbol{B} \cap \boldsymbol{C} \Rightarrow \boldsymbol{X}; \quad (4)$$

$$\boldsymbol{A} \cap \boldsymbol{D} \cap \boldsymbol{E} \Rightarrow \boldsymbol{X}. \quad (5)$$

IF

IOS versija pažeidžiama **AND**

konfigūracijoje yra komanda „webvpn gateway“ **AND**

komanda „interservice“

THEN

SSL VPN pažeidžiamumas CVE-2009-00626 egzistuoja.

IF

IOS versija pažeidžiama **AND**

konfigūracijoje yra komanda „webvpn enable“ **ir (AND)**

komanda „trustpoint“

Tada (THEN)

SSL VPN pažeidžiamumas CVE-2009-00626 egzistuoja.

Formą supaprastinti gali būti naudinga dėl fakto, jog sistemai plečiantis, ją gali tapti sunku administruoti. Tačiau, kaip pašalinė pasekmė, atsiranda išvados teiginio dublikavimas.

Be AND ir OR operatorių dar naudojamas NOT operatorius, kuris efektyviai pertraukia faktų sekos tikrinimą.

$$\boldsymbol{A} \cap \neg \boldsymbol{B} \cap \boldsymbol{C} \Rightarrow \boldsymbol{X}. \tag{6}$$

```
<definition id="oval:org.mitre.oval:def:6919" version="3" class="vulnerability">
    <metadata>
      <title>Cisco IOS WebVPN/SSLVPN Multiple Denial of Service Vulnerabilities</title>
      <affected family="ios">
        <platform>Cisco IOS</platform>
      </affected>
      <reference source="CVE" ref_id="CVE-2009-0626" ref_url="http://"/>
      <description>The SSLVPN feature in Cisco IOS 12.3 through 12.4 allows remote attackers to
                   cause a denial of service (device reload or hang) via a crafted HTTPS packet.
      </description>
      <oval_repository>
    </metadata>
    <criteria operator="OR">
      <criteria operator="AND" comment="Cisco IOS meets CVE-2009-0626">
        <criterion comment="IOS vulnerable versions" test_ref="oval:org.mitre.oval:tst:11435"/>
        <criterion comment="config contains: webvpn gateway" test_ref="oval:org.mitre.oval:tst:11540"/>
        <criterion comment="config contains: inservice" test_ref="oval:org.mitre.oval:tst:10979"/>
      </criteria>
      <criteria operator="AND" comment="Cisco IOS meets CVE-2009-0626">
        <criterion comment="IOS vulnerable versions" test_ref="oval:org.mitre.oval:tst:11435"/>
        <criterion comment="config contains: webvpn enable" test_ref="oval:org.mitre.oval:tst:10989"/>
        <criterion comment="config contains: ssl trustpoint" test_ref="oval:org.mitre.oval:tst:10990"/>
      </criteria>
    </criteria>
  </definition>
```

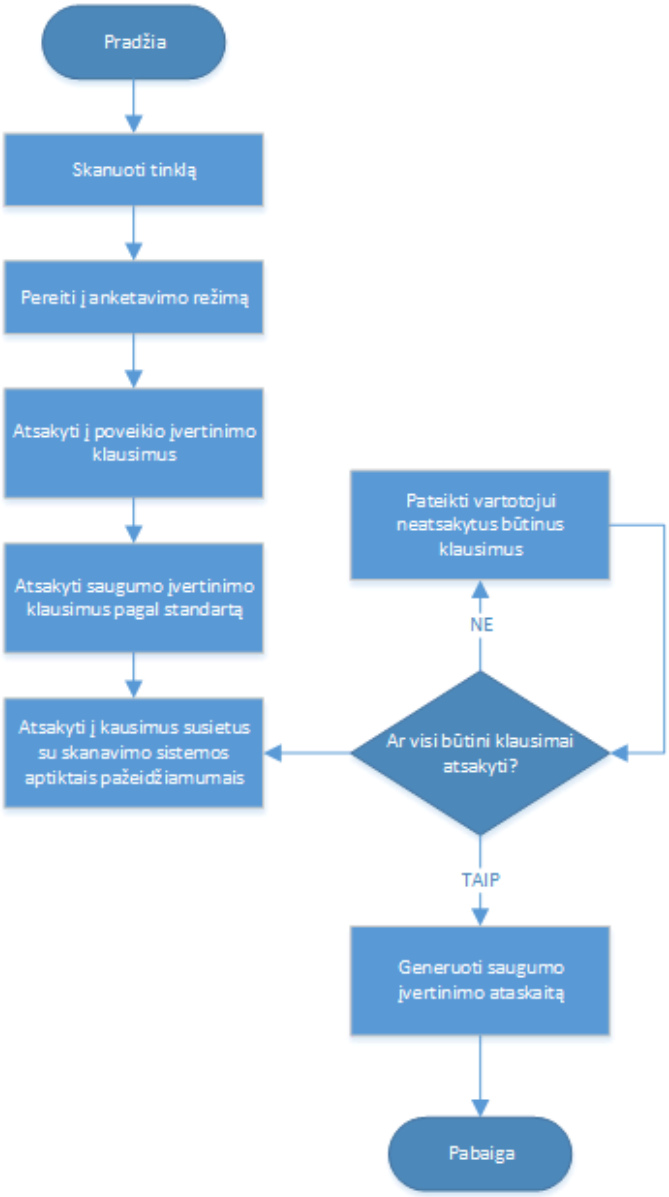
8 pav. Cisco SSL VPN pažeidžiamumo aprašas OVAL kalba (Dalis nebūtinų eilučių yra sutrauktos skaitomumo palengvinimui)

OVAL kalbos pasirinkimas diktuoja skanavimo sistemos, sugebančios interpretuoti tinklo įrangos aprašus, parašytus OVAL kalba, pasirinkimą. Turime pastebėti, kad OVAL duomenų bazėje yra gerokai daugiau aprašų, skirtų galiniams mazgams: Windows ar Unix šeimos serveriams ir darbinėms stotims. Ryškesnis kiekis pažeidžiamumų aprašų sukurtas tik Cisco IOS operacinę sistemą naudojančiai tinklo įrangai. Papildomai turime atsižvelgti ir į skanavimo įrankius: ne visi gali

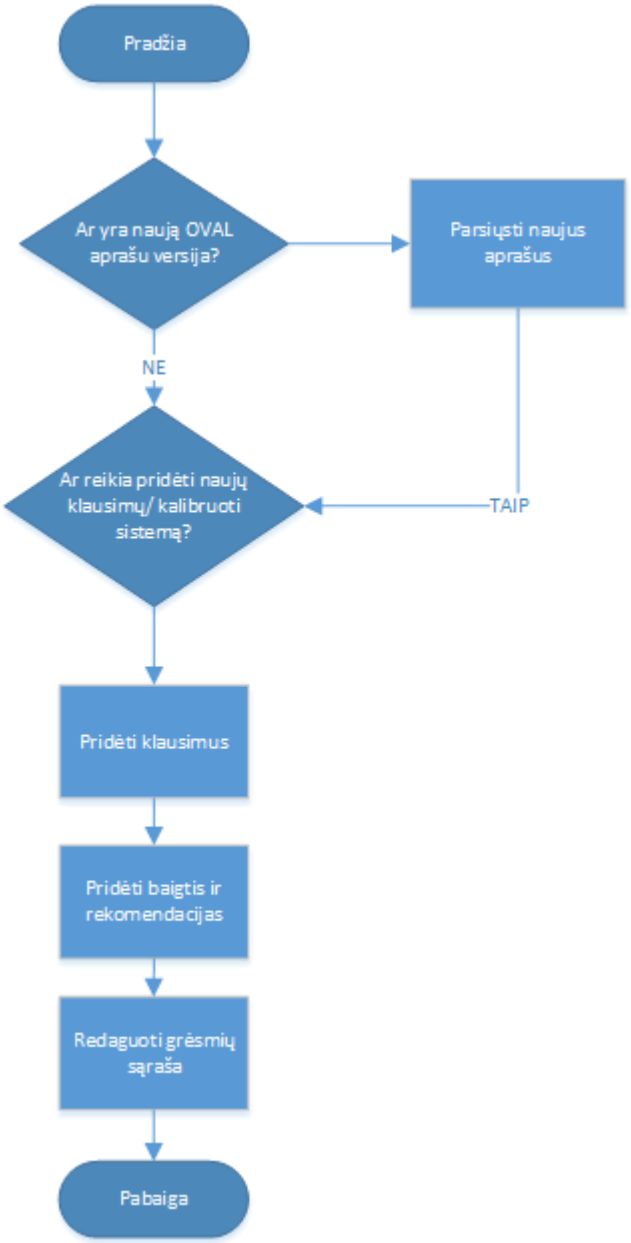
ištestuoti tinklo įrangos aprašus. Šiuo atveju pasirinksime analizės dalyje aprašytą jOVAL tinklo skanavimo įrankį. Pasirinkimą nulemia:

- Galimybė interpretuoti OVAL Cisco IOS pažeidžiamumų aprašus;
- Skaneris neapkrautas papildomais elementais, beveik nėra pašalinio, mums nebūtino funkcionalumo;
- jOVAL yra atviro kodo projektas;
- Skanavimo rezultatai atiduodami OVAL struktūrą atitinkančiais XML failais, tai palengvina tolimesnę integraciją.

Pačios ekspertinės sistemos panaudojimas yra sąlyginai nesudėtingas vartotojui: nereikia jokių programavimo ar specifinių su sistema susietų įgūdžių. Tačiau vartotojas turi būti pakankamai kvalifikuotas ir susipažinęs su įmonės infrastruktūra, kad atsakytų į užduodamus klausimus.



9 pav. Saugumo patikros procesas



10 pav. Sistemos papildymo OVAL aprašais ir klausimais procesas

3.2. Ekspertinės sistemos pasirinkimas

Darbe naudosime vieną iš egzistuojančių ekspertinės sistemos apvalkalų. Apvalkalą dažniausiai sudaro Rete algoritmo įgyvendinimas su papildomais įrankiais ar bibliotekomis, palengvinančiomis ekspertinių sistemų kūrimą. Apžvelgtos sistemos:

Drools – tai atviro kodo Rete algoritmu paremtas ekspertinės sistemos apvalkalas. Drools parašytas naudojant Java. Pagrindinės apvalkalo savybės:

- Rete algoritmas;
- Tiesioginės grandinės metodas;
- Drools apvalkalas yra gerai dokumentuotas ir aktyviai palaikomas;
- Taisykles galima aprašyti XML formatu.

OpenExpert – tai PHP kalba parašyta ekspertinė sistema, kuri gali būti naudojama kaip šablonas kitų sistemų kūrimui. Pagrindinė sistemos paskirtis yra teisinių patarimų suteikimas, tačiau dėl universalaus pateikimo sistemą galima lengvai pritaikyti kitoms ekspertinėms sistemoms. Sistemos savybės:

- Pilnai išvystyta vartotojo sąsaja;
- Palyginti su kitomis apžvelgtomis sistemomis, sistema yra pakankamai paprasta: žinias įvesti gali jokių papildomų IT sugebėjimų neturintis vartotojas, sistema nenaudoja sudėtingų palyginimo algoritmų, tokių kaip Rete.
- Sistema sunkiai išplečiama. Dėl palyginimo algoritmo trūkumo, ryšiai tarp klausimų ir atsakymų yra apibrėžiami statiškai. Sistemos bandymų metu, didėjant klausimų skaičiui, tapo vis sunkiau apibrėžti ryšius.

C Language Integrated Production System (CLIPS) – tai C kalba parašytas ekspertinių sistemų apvalkalas. CLIPS yra vienas plačiausiai paplitusių apvalkalų, parašytas 1985, juo paremta daug kitų vėliau sukurtų apvalkalų, tokių kaip Jess.

JESS – taisyklėmis paremtas apvalkalas. JESS yra Java kalba parašytas apvalkalas. JESS sukurtas CLIPS pagrindu. Savybės:

- Naudoja Rete algoritmą;
- Tiesioginės grandinės metodas;
- Taisykles galima aprašyti XML formatu;
- Žinias galima aprašyti taisyklėmis ir predikatų logika.

Pychinko yra Python kalba parašytas ekspertinių sistemų apvalkalas. Tai dar vienas Rete algoritmo įgyvendinimas, naudojant tiesioginės grandinės metodą. Apvalkalas orientuotas į mažai resursų turinčias sistemas, kurios gali būti nepajėgios naudotis kitais, sudėtingesniais apvalkalais paremtomis sistemomis. Savybės:

- Mažos apimties ir paprastas (apie 1400 kodo eilučių);
- Reikalaujantis mažai resursų;
- Rete algoritmas;
- Tiesioginės grandinės metodas.

3.3. Drools panaudojimas

Realizacijai pasirenkame Drools [20], pasirinkimą nulemia:

- Aktyvus sistemos palaikymas;
- Plati dokumentacija;
- Galimybė naudoti vieną iš keleto papildinių, tarp kurių yra Tohu sąsajos generavimo karkasas.

Drools žinių aprašymas nėra visiškai artimas žmogiškajai kalbai, tačiau taip pat nereikalauja itin specializuotų programavimo žinių. Naudojama MVEL skriptų rašymo kalba, skirta su Java parašytoms programoms. Daugumos taisyklių ir faktų aprašymas seka panašų šabloną:

```
Rule "CC1_8"
dialect "mvel"
no-loop
when
      $group : Group (id == "CC1");
then
      MultipleChoiceQuestion aMultipleChoiceQuestion = new
MultipleChoiceQuestion("CC1_8");
      aMultipleChoiceQuestion.setAnswerType(Question.TYPE_TEXT);
      aMultipleChoiceQuestion.setPreLabel("8. Įgyvendinkite tinklo
prieigos kontrolę (angl. Network Access Control arba NAC), kad galėtumėte
stebėti autorizuotas sistemas ir, pastebėjus ataką, galėtume perkelti
nepatikimą sistemą į virtualų tinklą (VLAN) su minimalia prieiga. Ar
tokios priemonės yra įgyvendinamos jūsų tinkle?");
      aMultipleChoiceQuestion.setPossibleAnswers({
            new PossibleAnswer(null, "Pasirinkite. . ."),
            new PossibleAnswer("Taip", "Taip"),
            new PossibleAnswer("Ne", "Ne")});
      insertLogical(aMultipleChoiceQuestion);
end
```

3.4. Standarto pasirinkimas

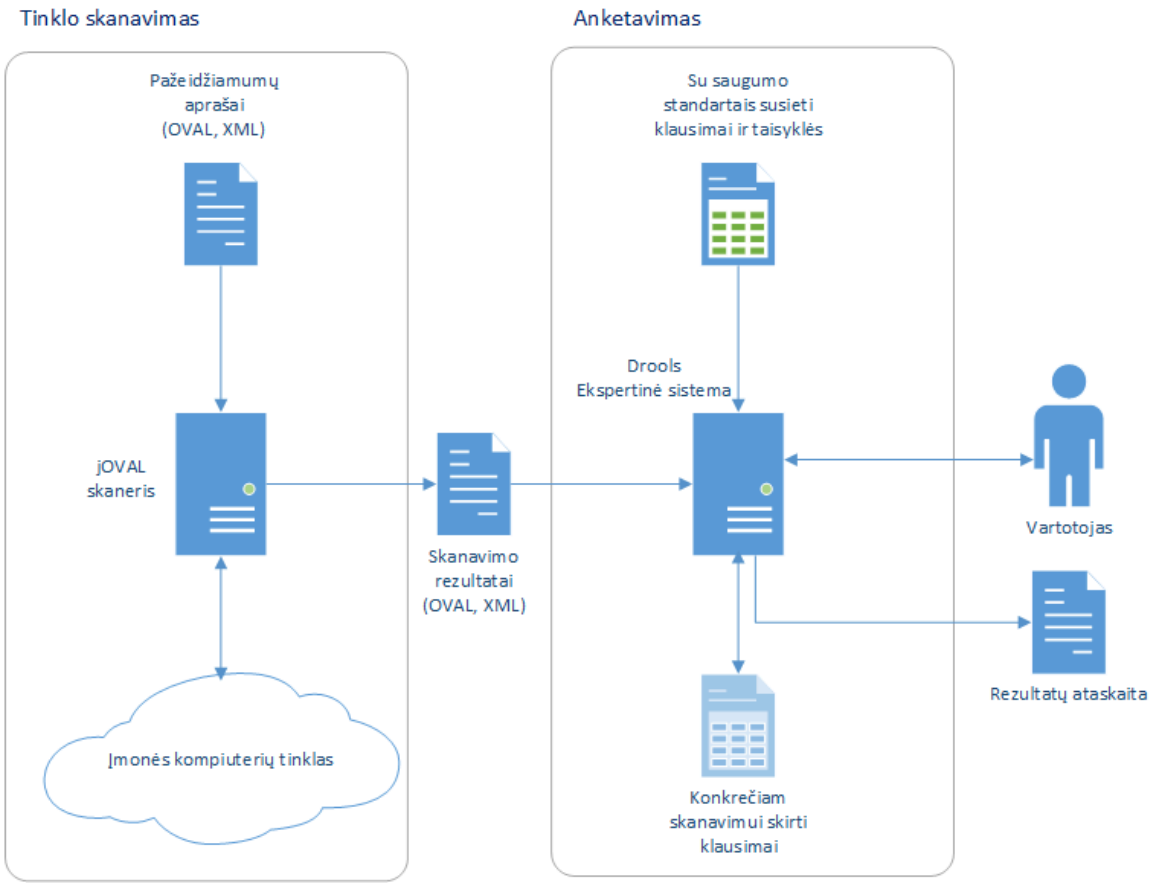
Norėdami nuosekliai įvertinti tinkle egzistuojančias kontrolės priemones ir surastus pažeidžiamumus, turime pasirinkti tokį saugumo standartą, pagal kurį vertinsime padėtį. Saugos kontrolinėms priemonėms apibrėžti paplitę keli standartai: ISO 27002, NIST 800-53, SANS 20 Critical Controls. Tinklo įvertinimui pasirenkame SANS 20 Critical Controls.

Šio standarto pasirinkimą sąlygoja standarto glaustumas, aiškus fokusavimas ir prioritzacija. Kritinės ir greitai sukuriamos kontrolės priemonės išskiriamos iš kitų, sunkiau įgyvendinamų ir bendrais atvejais turinčių ne tokį palankų resursų sąnaudų ir saugumo vertės santykį.

Reikia pastebėti, kad kito standarto pasirinkimas ir įgyvendinimas nėra techniškai apribotas. Esant reikalui SANS: 20 Cirtical Security Controls gali būti nesunkiai pakeistas bet kuriuo kitu standartu ar papildytais klausimais iš geriausių praktikų rinkinių. Standartų ir geriausių praktikų rinkinių derinys suteiktų papildomą granuliškumą, kur kritiniai saugumo punktai išplečiami rekomendacijomis ir praktiniais įgyvendinimo patarimais.

4. EKSPERTINĖS SISTEMOS REALIZACIJA

Sistemos prototipo realizacija remiasi kertine ekspertinės sistemos dalimi – taisyklių generatoriumi Drools, kuris yra įgyvendintas naudojant Java kalbą. Siekdami supaprastinti sąsajos sudarymo procesą, pasinaudojame Drools sistemai skirtu Tohu karkasu [18]. Tohu padeda iš taisyklių dinamiškai generuoti galutiniam vartotojui lengvai suprantamą grafinę sąsają. Sprendimo dalyje pateikėme bendrinę koncepcinę panašios sistemos schemą, kurią išplėtojame toliau (11 pav.).



11 pav. Papildyta ekspertinės sistemos realizacijos koncepcija, parodanti modulinę sandarą

jOVAL veikia atitinkamai kaip ir dauguma kitų OVAL kalba besinaudojančių skanavimo priemonių. Skaneriui reikia pateikti standartizuotą OVAL dokumentą su pažeidžiamumų ir testų, skirtų tiems pažeidžiamumas aptikti, aprašais. jOVAL apdoroja konfigūracijos informaciją prisijungęs prie įrenginio SSH protokolu arba naudodama lokaliai parsiųstus IOS konfigūracijos failus (.cfg). Rezultatai gali būti pateikiami tiek vartotojui įskaitomu html formatu, tiek kitoms sistemoms toliau apdoroti skirtu OVAL XML failu.

Konkrečiu atveju rezultatams kaupti nėra naudojamos duomenų bazės, rezultatai kaupiami XML formatu. OVAL kalba parašytas XML failas yra universalus ir suprantamas kitiems šios kalbos pagrindu veikiantiems įrankiams. Nereikia įdiegti ir palaikyti duomenų bazės, kurti atskiro metodo importuoti ir eksportuoti duomenims.

Drools taisyklės laikomos DRL formato failuose ir Excel darbalapiuose. Vieną darbalapį naudojame pastoviosios, nuo skanerio rezultatų nepriklausomos dalies saugojimui. Skaneriui perdavus duomenis, pastoviųjų taisyklių failas nuskaitomas, iš skanerio gauti duomenys paverčiami papildomomis taisyklėmis, kurios sujungiamos su jau egzistuojančiomis, ir įrašomos į naują.

Tohu pagalba iš darbalapio generuojama vartotojo sąsaja, kurioje užduodami visi klausimai. Pabaigus anketą, generuojama rezultatų atskaita.

4.1. Klausimynas

Vartotojo sąsajai kurti naudojamas Tohu karkasas. Jis įgalina taisyklių įvedimą XLS formatu ir išvedimą dinaminio puslapio pagalba, pasinaudojant JSP ir Java servletais.

Item ID	Type	Depends on Item ID	Attribute	Operation	Value	Data Type
	Page					
	Group					
	Question					Text
	Question					Text
	Group					
	MultipleChoiceQuestion					Text
	MultipleChoiceQuestion					Text

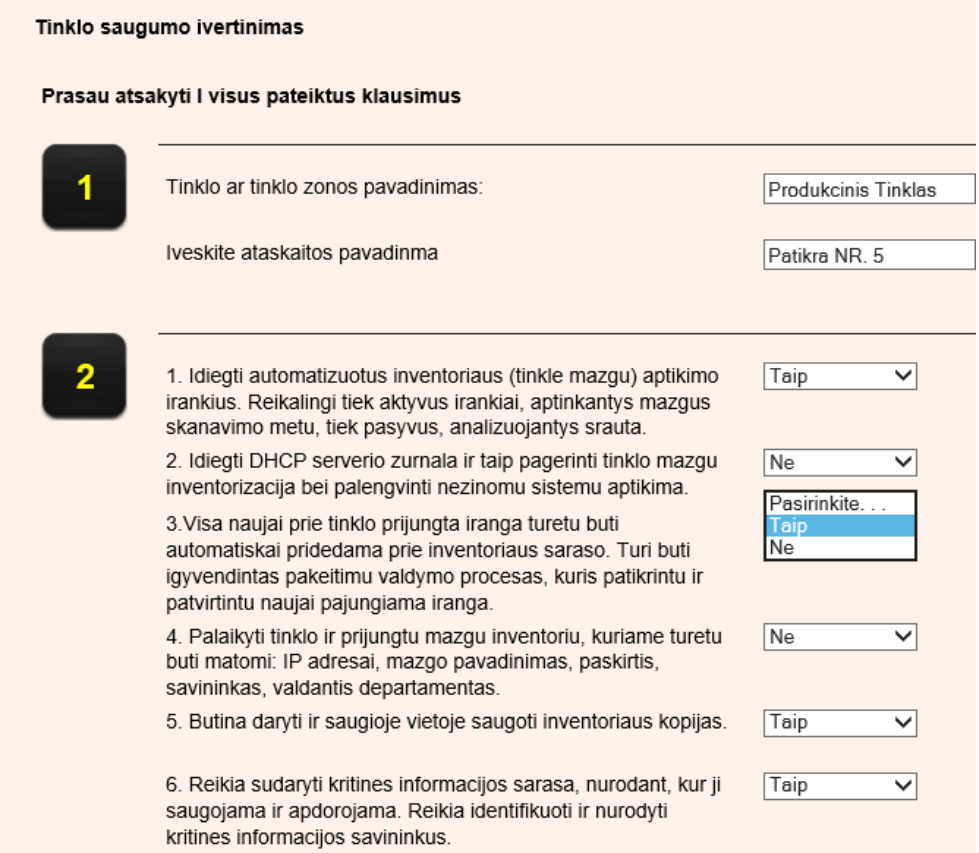
12 pav. Taisyklių įvedimo darbalapio dalis (Kai kurie laukai yra nematomi siekiant palengvinti skaitomumą)

4 lentelė Taisyklių darbalapio laukų paaiškinimas

Item ID	Klausimo ar rezultato, ar kito žinių elemento pavadinimas.
Type	Galimi įvairūs žinių elementų tipai: įvairaus tipo klausimai, išvados, grupavimo elementai.
Depends on Item ID	Nurodo klausimų/taisyklių tarpusavio priklausomybę.
Attribute	Žinių elementas ar atributas palyginimui.
Operation	Su atributu atliekama operacija: palyginimas (lygu, daugiau, mažiau), reikšmės įvertinimas pagal taisykles ir pan.
Value	Įvedama reikšmė, su kuria lyginamas atributas: kintamasis, statinė skaitinė ar tekstinė reikšmė, loginės true/false vertės.
Data Type	Klausimo ar atsakymo duomenų tipas: tekstas, data, loginės vertės.

Tokio tipo sąsaja žymiai sumažina programos įsisavinimo laiką. Palyginus su įvedimu naudojant MVEL, sumažėja įvesties dydis ir sudėtingumas. Vartotojui nereikia būti susipažinus su kalbos sintakse, didelė dalis vartotojų jau yra susipažinusi su darbalapiais ir jų valdymu.

Vizualiai sąsaja apipavidalinama įterpiant css failus, toks atskyrimas įgalina lengvą sistemos išvaizdos modifikavimą. Drools ir Tohu paremtoje sistemoje simboliai, nepriklausantis lotyniškam alfabetui, įskaitant ir lietuviškus, sukelia sistemos nestabilumą/yra prarandami konvertavimo metu.



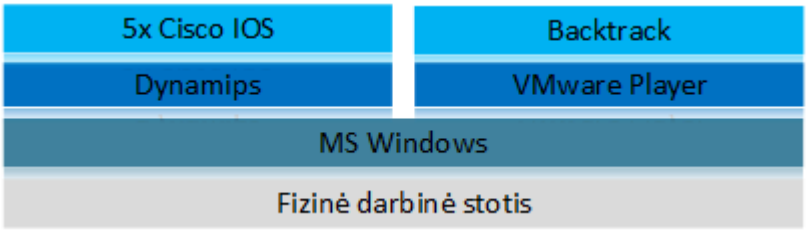
13 pav. Tohu karkaso pagalba iš darbalapių generuojama sąsaja. Apklausos lango pavyzdys

Drools leidžia apklausas paversti dinamiškomis, jei netenkinamos būtinos klausimo sąlygos, klausimas išvis nėra užduodamas.

4.2. Tiriamas tinklas

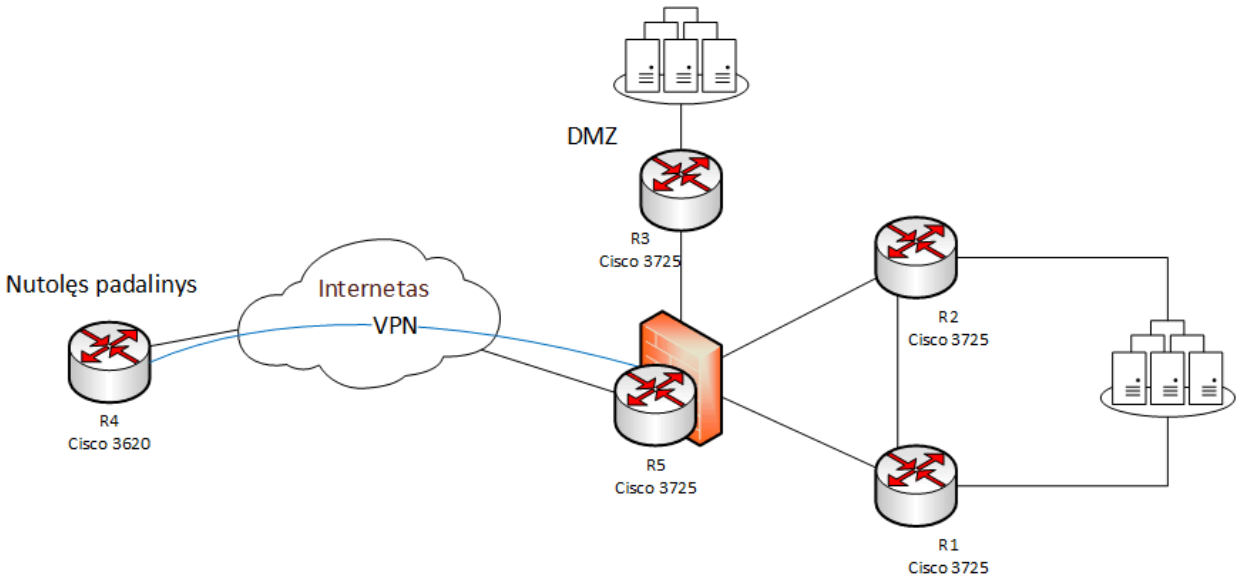
Siekiant sukurti kontroliuojamą aplinką su apibrėžtais kintamaisiais, bus tiriamas virtualus šiai užduočiai sukurtas tinklas. Virtualus tinklas leidžia sukurti daug lankstesnę infrastruktūrą, neapribotą produkciniams tinklams būdingų limitų.

Tinklas virtualizuotas pasinaudojant Dynamps virtualizacijos sprendimu, kuris yra skirtas ne tik virtualizuoti atskirtų tinklo įrenginių operacines sistemas, bet ir viso tinklo darbą. Prie šios virtualizuotos aplinkos, naudojantis virtualia sąsaja, prijungta reali darbinė stotis su tokiomis programomis kaip NMAP ir jOVAL. Atskirai, naudojantis VMware sprendimu, virtualizuota Backtrack sistema. Backtrack – tai Linux šeimos pagrindu sukurta sistema, skirta saugumo testavimui, spragų tyrimui ir įsilaužimų testavimui. VMware aplinka taip pat virtualios sąsajos pagalba prijungta prie virtualaus tinklo.



14 pav. Darbe naudojamos aplinkos virtualizacijos sluoksniai

Tinklo infrastruktūra sudaryta taip, kad leistų išbandyti kuo daugiau saugumo scenarijų: kelios skirtingo saugumo lygių zonos, VPN, keli skitingų modelių maršrutizatoriai. Vietoje dedikuotos ugniasienės naudojame maršrutizatorių su aprašytomis adresų filtravimo taisyklėmis. Nedidelius resursus turinčios įmonės dažnai pasirenka „viskas viename“ sprendimus ir neįgyvendina dedikuotų ugniasienių. Tinklas gali būti suskirstytas į tris pagrindines zonas: patikimą vidinį tinklą, nepatikimą išorinį tinklą (internetą) ir iš dalies patikimą tinklą (DMZ). Reikėtų pastebėti, kad nėra sumodeliuota OSI L2 sluoksnio komutatorių. Priklausomai nuo skanavimo parametrų, komutatoriai gali būti išvis nematomi. Šiuolaikiniai komutatoriai komutavimo procesą atlieka fizinėje techninėje įrangoje, ASIC grandinėse, kurių negalima virtualizuoti dabartinėmis priemonėmis. Nors komutatoriai gali turėti specifinių pažeidžiamumų (STP, VTP atakos, VLAN pakeitimo atakos ir pan.), daroma prielaida, kad tyrimui užtenka L3 įrenginių, nes spragų aptikimas ir saugumo analizė komutatorių atžvilgiu būtų atliekama analogiškai.



15 pav. Darbe naudojamo virtualaus tinklo topologija

5 lentelė Virtualios tinkle infrastruktūros paaiškinimai ir komentarai

Tinklo mazgo vardas	Tipas	Virtualios tech. įrangos versija	OS versija	Paskirtis / Komentarai
R1	Maršrutizatorius	Cisco 3725	IOS 12.3(4)T4	Vidinis tinklo maršrutizatorius. Naudoja dinaminio maršrutizavimo protokolą: EIGRP
R2	Maršrutizatorius	Cisco 3725	12.4(3)	Vidinis tinklo maršrutizatorius Naudoja dinaminio maršrutizavimo protokolą: EIGRP
R3	Maršrutizatorius	Cisco 3725	12.4(3)	DMZ zonoje esantis maršrutizatorius. Prieiga iš kitų tinklo dalių yra ribojama ACL.
R4	Maršrutizatorius	Cisco 3620	IOS 12.2(2)T	Maršrutizatorius, naudojamas pajungti nutolusiam įmonės padaliniui, naudojant IPSec VPN tunelį, per internetą. Sukonfigūruotas VPN tunelis.
R5	Maršrutizatorius	Cisco 3725	IOS 12.3(4)T4	Maršrutizatorius, naudojamas vietoje ugniasienės. ACL pagalba atskiria internetą, dalinio patikimumo tinklą (DMZ) ir patikimą vidinį tinklą. Sukonfigūruota FTP paslauga. Sukonfigūruotas VPN tunelis.

5. EKSPERIMENTINIS TINKLO TYRIMAS

5.1. Skanavimai

Suplanuojami ir atliekami keletas skanavimo bandymų, siekiant palyginti gaunamus rezultatus, jų išsamumą bei panaudojamumą, kuriant hibridinės ekspertinės sistemos prototipą. Taip pat skanavimo metu siekiama aptikti ir dokumentuoti iš anksto nenumatytus pažeidžiamumus, kurie nebuvo specialiai suprojektuoti. Tokie papildomi pažeidžiamumai gali būti aptikti dėl operacinės sistemos versijos, pataisymų trūkumo ar tinklo modelio įgyvendinimo spragų.

1. Bandymas:

Tinklas skanuojamas NMAP skenerių. Skanavimas gali būti vertinamas kaip trikdantis, neautentifikuotas, triukšmingumas priklauso nuo pasirinkto skanavimo metodo (TCP SYN, TCP Connnect ir pan.). Reiktų pastebėti, kad testuojamas tinklas neturi IPS/IDS sistemos. Dėl to realų triukšmingumo lygį įvertinti sudėtinga. Šiuo atveju panaudojamas NMAP intensyvaus skanavimo profilis:

.nmap -T4 -A -v 192.168.0.0/24, 172.16.0.0/24, 10.0.0.0/24, 10.0.0.1 (1)

Opcija „–A“ įjungia OS aptikimą, versijos aptikimą, paleidžia NMAP skanavimo skriptus. Nors tikslūs tinkle mazgų adresai yra žinomi, naudojame didesnius įmonės tinklų adresus. Taip patikriname NMAP galimybę sėkmingai aptikti visus mazgus ir naudojame kaip priemonę surasti aktyvius mazgus.

Bandymo rezultatai:

Mazgai ir prievadai aptinkami greitai ir efektyviai, tačiau OS versijos aptinkamos tik apytiksliai:

R1 mazgo OS detalės matomos NMAP skaneryje:

OS details: Cisco 2900-series, 3650, or 3750 switch; 6509 or 7206VXR router; or uBR925 or uBR7111 cable modem (IOS 12.1 - 12.2)

Įrenginio operacinėje sistemoje pateikiama reali informacija:

R1#sh ver

Cisco IOS Software, 3700 Software (C3725-ADVENTERPRISEK9-M), Version 12.3(4)T4, RELEASE SOFTWARE (fc2)

Nors NMAP, naudodamasi operacinės sistemos antspaudu, versiją aptiko gana tiksliai, toks tikslumas gali būti nepakankamas.

Darbo rašymo metu, Cisco IOS 12.1 ir IOS 12.2 turi po 60 registruotų bendrų pažeidžiamumų [21], tačiau jų kiekis gali skirtis nuo pataisymo versijos. Dalis pažeidžiamumų sutaps su 12.3 versijos pažeidžiamumais, tačiau sistemos versijos netikslumas iškreipia tyrimą ir padidina paieškos plotą nuo 60 galimų pažeidžiamumų iki 120.

R1 žurnale matome įrašus, sukeltus skanavimo veiksmų.

R2#

05:06:47: %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from 192.168.0.1

2. Bandymas:

Autentifikuotas skanavimas naudojantis OpenVAS sistema. Nors bendras pažeidžiamumų aprašų skaičius gana didelis, 2013 m. balandžio mėnesį sistemoje buvo prieinama virš 30 000 OpenVAS pažeidžiamumų testų (NVT), rezultatai yra nepatenkinami dėl mažo konkrečiai tinklo įrangai būdingus pažeidžiamumus aprašančių NVT testų skaičiaus.

Kontekste turime pastebėti, kad OpenVAS diegiama galimybė pasinaudoti ne tik NVT, bet ir OVAL testais, kas galėtų įgyvendinti OpenVAS panaudojimą panašioje sistemoje netolimoje ateityje.

3. Bandymas:

Autentifikuotas skanavimas naudojant OVAL pagrindu veikiančią jOVAL programą.

Programa išanalizuoja Cisco „*show tech-support*“ komandos rezultatus ir tiksliai aptinka operacinės sistemos versijas. Tai vienas iš svarbiausių kriterijų nustatant pažeidžiamumus.

System Information	
Host Name	R1
Operating System	Cisco IOS
Operating System Version	12.3(4)T4
Architecture	R7000

16 pav. jOVAL pateikti rezultatai atitinka realią sistemos versiją

Autentifikuotas skanavimas, palyginus su kitomis skanavimo priemonėmis, parodo pranašumą tikslumu ir tuo, kad visiškai nesukelia sistemos sutrikimų. Naudodamiesi jOVAL, ištiriame R1-R5 maršrutizatorius.

Reference ID	Title
CVE-2005-4437	Cisco "EIGRP" Protocol "HELLO" Packet Replay Vulnerability
CVE-2011-3279	The provider-edge MPLS NAT implementation in Cisco IOS 12.1 through 12.4 and 15.0 through 15.1, and IOS XE 3.1.xSG, allows remote attackers to cause a denial of service (device reload) via a malformed SIP packet to UDP port 5060, aka Bug ID CSCti98219
CVE-2006-3906	Cisco Multiple Products IKE Packet DoS
CVE-2005-1021	Cisco Systems IOS SSH Transmission Control Blocks DoS Vulnerability
CVE-2005-3481	Cisco IOS System Timers Heap Overflow Code Execution Vulnerability
CVE-2006-0354	Cisco Aironet Access Point ARP Memory Exhaustion DoS Vulnerability
CVE-2005-0195	Cisco Systems IOS IPv6 Heap Corruption Vulnerability
CVE-2005-3669	Cisco Systems Malformed IPSec IKE DoS Vulnerability
CVE-2007-0479	Cisco IOS IPv4 Memory Leak DoS Vulnerability
CVE-2007-0480	Cisco IOS IP Option Remote Code Execution Vulnerability
CVE-2006-4950	Cisco Systems Non-DOCSIS Platform Default DOCSIS SNMP Support Vulnerability
CVE-2005-1020	Cisco Systems IOS SSH2 DoS Vulnerability
CVE-2005-4436	Cisco "EIGRP" Protocol "Goodbye Message" Packet Replay Vulnerability

17 pav. Pažeidžiamumai gauti nuskanavus R1

R1, palyginus su R5, gaunamos tokios pačios klaidos. R5 išsiskiria tuo, kad teikia FTP (angl. *File Transfer Protocol*) paslaugą ir turi sukonfigūruotą VPN:

```
R5(config)#crypto isakmp policy 1
R5(config-isakmp)#encr 3des
R5(config-isakmp)#hash md5
R5(config-isakmp)#authentication pre-share
R5(config-isakmp)#group 2
R5(config-isakmp)#lifetime 86400
R5(config-isakmp)#crypto isakmp key cisco address 10.30.0.2
```

R5 VPN jokio pažeidžiamumo neregistruoja, tačiau aptinkamas FTP pažeidžiamumas CVE-2007-2586.

oval:org.mitre.oval:def:6047	true	vulnerability	CVE-2008-3801	Cisco IOS Session Initiation Protocol Denial of Service Vulnerability
oval:org.mitre.oval:def:5927	true	vulnerability	CVE-2008-3799	Cisco IOS Session Initiation Protocol Denial of Service Vulnerability
oval:org.mitre.oval:def:5889	true	vulnerability	CVE-2008-3802	Cisco IOS Session Initiation Protocol Denial of Service Vulnerability
oval:org.mitre.oval:def:7123	true	vulnerability	CVE-2008-3806	Cisco 10000, uBR10012, uBR7200 Series Devices IPC Vulnerability
oval:org.mitre.oval:def:6086	true	vulnerability	CVE-2008-3800	Cisco IOS Session Initiation Protocol Denial of Service Vulnerability

18 pav. Unikalūs pažeidžiamumai, gauti nuskanavus R3

Tyrimui pasirenkame 5 pažeidžiamumus. Kai kurie kiti pažeidžiamumai gali būti greitai atmesti, nes sukurtame tinklo modelyje netenkinamos pradinės jų egzistavimo sąlygos. Skaneris šių sąlygų patikrinti negali, tačiau ekspertinė sistema, pridėjusi atitinkamas žinias, tokius pažeidimus gali atmesi uždavusi vieną ar du bazinius klausimus.

Toliau nenagrinėjamų pažeidžiamumų sąrašas:

6 lentelė Nenagrinėjamų pažeidžiamumų sąrašas

CVE numeris	Aprašas	Komentaras
CVE-2006-0354	Cisco Aironet prieigos taško (angl. Access Point arba AP) ARP atminties užpildymo pažeidžiamumas.	Darbe nenaudojama įranga; bendruoju atveju pažeidžiamumą galima atmesti vieno/dviejų klausimų pagalba: • Ar naudojamas bevielis tinklo ryšys? • Ar naudojamas Aironet AP?
CVE-2006-4950	Data Over Cable Service Interface Specification (DOCSIS) telekomunikacijos standarto pažeidžiamumas.	Nenaudojami įrangos tipai. Sprendimas analogiškas CVE-2006-0354 Aironet pažeidžiamumo atpažinimui.
CVE-2005-0195	DoS ataka naudojantis modifikuotais IPv6 paketais.	Sumodeliuotame tinkle IPv6 nėra naudojamas. Nenaudojant IPv6 protokolo, apdorojimas turėtų būti išjungtas ar užblokuotas ACL.
CVE-2011-3279	MPLS NAT įgyvendinimo spragos Cisco IOS versijose 12.1 - 12.4 leidžia nuotoliniu būdu atlikti DoS ataką (įrenginio perkrovimus), naudojantis blogai suformuotu SIP paketu, nukreiptu į UDP 5060 prievadą.	Spraga praktiškai nėra išnaudojama, nebent įmonė naudoja MPLS. Tokiu atveju, reikia išjungti SIP paketų transliavimą: **no ip nat service sip udp port 5060**
CVE-2005-1020 / CVE-2005-1021	DoS atakos, naudojantis SSH spragomis, įmanomos tik kai autentifikacijai naudojamas TACACS+ serveris.	Tinklo modelyje naudojama tik lokali autentifikacija.

Taip pat egzistuoja kelios grupės analogiškų CVE aprašų, tiek aptikimo, tiek sprendimo atžvilgiu beveik identiški pažeidžiamumai, kurie gali būti tiriami kaip viena bendra spraga:

- CVE-2007-0479 ir CVE-2007-0480: DoS atakos, naudojantis modifikuotomis IPv4 paketo antraštėmis.
- CVE-2005-1020 ir CVE-2005-1021: DoS atakos, naudojantis SSH spragomis, įmanomos tik kai autentifikacijai naudojamas TACACS+ serveris.
- CVE-2005-4436 ir CVE-2005-4437 EIGRP maršrutizavimo pažeidžiamumai DoS atakoms.

CVE-2005-3481: Bendrinės buferio perpildymo atakos, savaime nėra pažeidžiamumas, tai silpna dizaino vieta, kuri gali padėti išnaudoti kitus pažeidžiamumus.

CVE-2006-3906: Daugybiniai pažeidžiamumai DoS atakoms Internet Key Exchange Version 1 (IKEv1) protokole. Gali būti vertinama kaip bendra protokolo dizaino problema.

7 lentelė Tiriamų pažeidžiamumų sąrašas

Mazgas:	CVE	Aprašas	CVSS
R1-R5	CVE-2005-4437	Extended Interior Gateway Routing Protocol (EIGRP) MD5 kaimyninių mazgų autentifikavimo spraga. EIGRP nuo Cisco IOS 11.3 versijos nebeprideda žinutės autentifikavimo kodo (angl. Message Authentication Code arba MAC) į paketo vientisumo patikrinimą. Tai leidžia piktavaliams iš paketų nuskaityti maišos funkcijas ir jomis pasinaudojant išsiųsti didelį kiekį EIGRP „*hello*“ žinučių arba išsiųsti didelį kiekį EIGRP „*neighbour announcement*“, taip sukeliant ARP (angl. *Address Resolution Protocol*) paketų audrą lokaliame tinkle.	7.5
R1-R5	CVE-2005-4436	EIGRP protokolo „*Goodbye Message*“ paketo pakartojimo pažeidžiamumas. EIGRP 1.2 versijos įgyvendinimas vėlesnėse nei 12.3(2), 12.3(3)B ir 12.3(2)T OS versijoje leidžia nuotoliniu būdu sukelti DoS ataką, pasinaudojant nevienodomis protokolo „k“ vertėmis arba „*Goodbye message*“ parametru Type-Length-Value (TLV).	7.8
R5	CVE-2007-2586	Cisco IOS FTP serverio autentifikacijos apėjimo pažeidžiamumas. IOS FTP serveris tinkamai nepatikrina prisijungimo duomenų, dėl ko įmanoma įvykdyti kodo įterpimo ataką.	9.3
R1, R4-R5	CVE-2007-0479/ CVE-2007-0480	Pirmuoju atveju vykdomos DoS atakos, naudojantis modifikuotomis IPv4 paketo antraštėmis. Antruoju, CVE-2007-0480 piktavaliai gali įterpti pasirinktą kodą.	7.8/ 10.0

Norint juos ištirti ir suvaldyti, ekspertinėje sistemoje reikia pažeidžiamumus susieti su kontrolės klausimais.

8 lentelė Pažeidžiamumų kontrolės priemonės

CVE	Kontrolinės priemonės	Pažeidžiamas konfigūracijos elementas
CVE-2005-4436 / CVE-2005-4437	Galimi rizikos sumažinimo sprendimai [19]: - Priėjimo į tranzitinį tinklą blokavimas, pasinaudojant ACL (angl. *Access Control List*) filtrais. Daugumai vartotojų niekada nereikia jungtis į potinklius, skirtus maršrutizatoriams. - Sukonfigūruoti adresų patikrinimą (angl. *anti-spoofing*) perimetro įrangoje. - 802.1x protokolu paremtas tinklo mazgų autentifikavimas. - MD5 EIGRP kaimyninių mazgų autentifikavimas.	router eigrp 1 redistribute static passive-interface FastEthernet0/1 network 10.0.0.0 network 172.16.0.0 auto-summary
CVE-2007-0479/ CVE-2007-0480	Pažeidžiamumas kritinis, dėl šio pažeidžiamumo nevykdyti tolesnių apklausų, iškart primygtinai pasiūlyti įdiegti stiprius ACL: • Echo (Ping) ICMP type 8 • Timestamp ICMP type 13 • Information Request ICMP type 15 • Address Mask Request ICMP Type 17 • Protocol Independent Multicast (PIM) IP protocol 103 • Pragmatic General Multicast (PGM) IP protocol 113 • URL Rendezvous Directory (URD) TCP port 465 Atnaujinti OS versiją į 12.4 ar kitą rekomenduojama gamintojo.	Programinės įrangos pažeidžiamumas
CVE-2007-2586	Vartotojui pateikiama rekomendacija naudotis kitais būdais failams persiųsti.	Pažeidžiamumas Cisco IOS FTP įgyvendinime ftp-server enable komanda

Radus EIGRP CVE-2005-4437 pažeidžiamumą, aktyvuojami ir užduodami kontroliniai klausimai, tokie kaip: „CVE-2005-4437 – rizikos įvertinimas. Ar naudojate ACL apsaugoti tranzitinius tinklo infrastruktūros potinklius?“.

CVE-2005-4437 ACL klausimas MVEL formoje:

```
when

      $group : Group (id == "CVE-2005-4437_questions");

then

      MultipleChoiceQuestion aMultipleChoiceQuestion = new
MultipleChoiceQuestion("IMPQ1_1");

      aMultipleChoiceQuestion.setAnswerType(Question.TYPE_TEXT);

      aMultipleChoiceQuestion.setPreLabel("CVE-2005-4437 rizikos
ivertinimas Ar naudojate ACL apsaugoti tranzitinius tinklo
infrastrukturos potinklius?");

      aMultipleChoiceQuestion.setPossibleAnswers({

            new PossibleAnswer(null, "Pasirinkite. . ."),

            new PossibleAnswer("Taip", "Taip"),

            new PossibleAnswer("Ne", "Ne")});

      insertLogical(aMultipleChoiceQuestion);

end
```

Tinklo modelyje tokie ACL nėra suplanuoti, pateikiamas neigiamas atsakymas.

Taip pat panaudojami ir bendri teiginiai iš SANS: 20 Critical Security Control standarto, į kuriuos galima atsakyti taip arba ne:

„7. Panaudokite 802.1x protokolą įrenginių prisijungimo prie tinklo valdymui. 802.1x turi būti susietas su inventoriaus sąrašu, kad galėtų atpažinti autorizuotas ir neautorizuotas sistemas.“

5.2. Tyrimo rezultatai

Iš atlikto tyrimo galime daryti išvadą, kad tinklo saugumo įvertinimas naudojantis ekspertine sistema yra iteracinis procesas. Vartotojo atliktus skanavimus seka tolimesni saugumo konsultanto/analitiko sistemos kalibravimo ir žinių pridėjimo veiksmai. Pirmųjų bandymų metu, sistemos efektyvumas ir spragų aptikimo galimybės yra lygios grynajam skanerio efektyvumui. Žinių

bazei pildantis, didėja galimybė užkirsti kelią pažeidžiamumui net kai jo skaneris ir neaptinka. Tam tikslui, šalia konkretiems pažeidžiamumams būdingų taisyklių, įkeliamos bendros taisyklės, kurios patikrina, kaip įmonės tinklas atitinka standartų keliamus reikalavimus ir geriausias praktikas.

Tyrimo metu nustatyta, kad skaneris, o kartu ir ekspertinė sistema, daug lengviau aptinka naujus pažeidžiamumus (iki poros metų senumo). Pats įrangos gamintojas Cisco nepateikia senesnių aprašų, kai kurie iš Mitre organizacijos pateiktų aprašų neatitiko šiandieninio standarto dėl pačios kalbos žymų evoliucijos.

Iš 13 rastų pažeidžiamumų sistema gali iškart atmesti 5 kaip klaidingus.

5.3. Tolimesni darbai

Rasti, ištirti ir parinkti efektyvų metodą pažeidžiamumų duomenų ir geriausių praktikų ir/ar saugumo kontrolės priemonių susiejimui.

Pasiūlyti metodą, kaip išreikšti pažeidžiamumų modifikuotas CVSS reikšmes, priklausomai nuo tinklo infrastruktūros ir esamų saugumo kontrolės priemonių.

Išplėsti automatizavimo metodus ir įgalinti kelių skanerių domenų koreliaciją, siekiant sumažinti klaidingų spragų aptikimo skaičių.

6. GALUTINĖS DARBO IŠVADOS

- Panaudojant tokias priemones kaip SCAP protokolas ar jo atskiri elementai (OVAL, CCE, CVE, CVSS), galima pateikti universalius modulinius produktus standartizuotomis sąsajomis, kurie gali būti išplečiami pagal poreikį.
- Mažų ir vidutinių įmonių niša gali būti potencialiai užpildyta SaaS principais pateikiamų įrankių, taip prisitaikant prie limituotų tokio segmento įmonių resursų.
- Automatizuotomis priemonėmis papildytą ekspertinę sistemą galima, neatliekant papildomų metodikos ar dizaino pakeitimų, išplėsti už tinklo saugumo domeno įvertinimo ribų.
- OVAL standartizavimo ir automatizavimo priemonės dar nepasiekė pilnos brandos, tinklų apsaugos srityje trūksta OVAL kalba parašytų aprašų ir juos naudoti galinčių įrankių, išimtis yra Cisco gaminama įranga, kuriai, darbo rašymo metu, buvo prieinama 140+ OVAL aprašų.
- Pagrindinė tokios sistemos limitacija: priklausomybė nuo žinių bazės atnaujinimo ir kalibravimo, tačiau net ir neatnaujinus tokios bazės sistema gali funkcionuoti naudodama nuo ekspertinės sistemos nepriklausančius OVAL pažeidžiamumų aprašus.
- Panaudojant automatizuotomis priemonėmis papildytą ekspertinę sistemą, identifikuotų pažeidžiamumų skaičių pavyko sumažinti daugiau kaip 35%, atmetant klaidingai identifikuotus ir konkrečiam tinklui neaktualius pažeidžiamumus.

7. LITERATŪRA

1. Verizon RISK Team 2012 Data Breach Investigations Report, 2012, p. 3.
2. Anantha Sayana S. Approach to Auditing Network Security. *Information Systems Control Journal*, 2003, vol. 5, p.
3. Harris Sh. CISSP All in One Exam Guide, 2013, p. 30.
4. Critical Controls for Effective Cyber Defense, version 4.1, 2013, p. 2.
5. The Standard of Good Practice for Information Security. *Information Secuirty Forum*, 2007, p. 65.
6. Chuvakin A. *Vulnerability and Security Configuration Assessment Solutions Comparison* [interaktyvus] [žiūrėta 2013-05-21] Prieiga per internetą: http://www.gartner.com/technology/media-products/reprints/qualys/Qualys_225382.html
7. Using an Expert System for Deeper Vulnerability Scanning. *Whitepaper, Rapid7.* 2012, p. 21
8. National Institute of Standards and Technology *The Open Checklist Interactive Language (OCIL)* [interaktyvus] [žiūrėta 2013-05-21] Prieiga per internetą: http://scap.nist.gov/specifications/ocil/
9. CISCO *Security Automation Using OVAL* [interaktyvus] [žiūrėta 2013-05-21] Prieiga per internetą: http://www.cisco.com/web/about/security/intelligence/oval_scty_automation.html
10. Krishnamoorthy C.S.; Rajeev S. Artificial Intelligence and Expert Systems for Engineers. *CRC Press LLC*, 1996, p. 37.
11. Chakraborty R.C. Expert systems: AI course. *Lecture 35-36*, slides 28-30.
12. Liu D.; Gu T.; Jiang-Ping X. Rule Engine Based on Improvement Rete Algorithm. *High Speed Institute of China Aerodynamics Research & Development Center*, 2011, p. 346.
13. Riley G.; Giarratano J. Expert Systems: Principles and Programming. 1998, p. 3-7.
14. Laudon K.; Laudon J.; Fimbel E. Information Systems: Managing the Digital Firm, Business & Economics, 2012, 12th edition, p. 434.
15. Open Vulnerability and Assessment Language *Repository* [interaktyvus] [žiūrėta 2013-05-21] Prieiga per internetą: http://oval.mitre.org/repository/
16. Xinming Ou A logic-programming approach to network security anglysis. *Princeton University*, 2005, p. 51.
17. Katz Y.; Parsia B.; Clark K.; Pychinko: A Native Python Rule Engine. *International Python Conference*, March 2005, Washington D.C. Prieiga per internetą: http://www.mindswap.org/~katz/Talks/2005/pycon/pychinko.pdf

18. Jackson R. and El-Sheikh E. A Case Study: Building a Web-Based Dietitian Expert System. *Department of Computer Science, University of West Florida*, p. 2.
19. CISCO *Full-Disclosure: Multiple Vulnerabilities within Cisco EIGRP* [interaktyvus] [žiūrėta 2013-05-21] Prieiga per internetą: http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20051220-eigrp
20. Gamal M. M., Dr. Hasan B. & Dr. Hegazy A. F. A Security Analysis Framework Powered by an Expert System. *Computer Science Arab Academy of Science, Technology and Maritime Transport, International Journal of Computer Science and Security (IJCSS)*, 2011, vol. 4, p. 514.
21. CVE Details *Cisco: Vulnerability Statistics* [interaktyvus] [žiūrėta 2013-05-21] Prieiga per internetą: http://www.cvedetails.com/vendor/16/Cisco.html

SANTRUMPŲ ŽODYNAS

ACL – Access Control List

IPS – Intrusion Prevention System

IDS – Intrusion Detection System

OSI – Open Systems Interconnection

RADIUS – Remote Authentication Dial In User Service

TACACS – Terminal Access Controller Access-Control System

ALE – Annual Loss Expectency

SLE – Single Loss Expectancy

ARO – Annual Rate of Occurrence

SCAP – The Standardof Good Practice for Information Security

ISMS – Information Security Management System

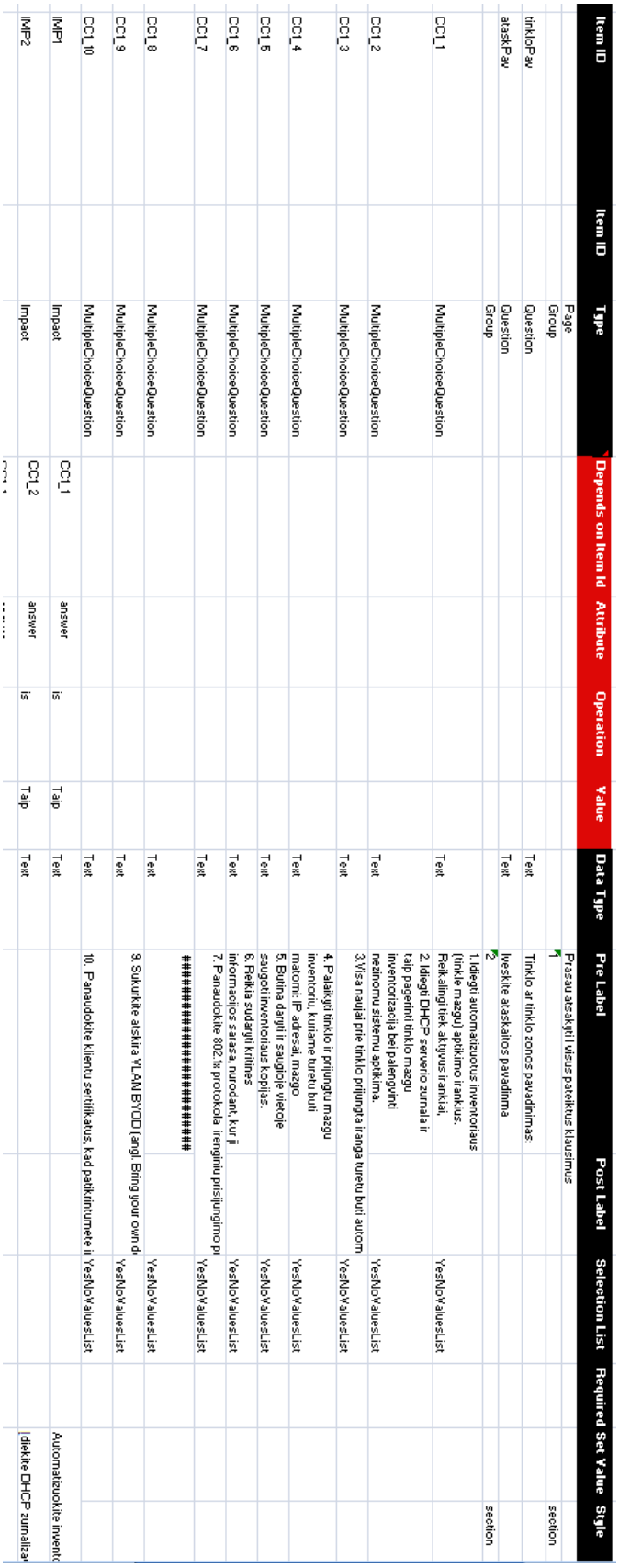
OVAL – Open Vulnerability Assessment Language

SCAP – Security Content Automation Protocol

SIEM – Security Information and Event Management

PRIEDAI

Priedas Nr.1



Item ID	Item ID	Type	Depends on Item Id	Attribute	Operation	Value	Data Type	Pre Label	Post Label	Selection List	Required	Set Value	Style
		Page						Prasau atsakyti į visus pateiktus klausimus					
		Group						1					section
tinkloPav		Question					Text	Tinklo ar tinklo zonos pavadinimas:					
ataskPav		Question					Text	Iveskite ataskaitos pavadinima					
		Group						2					section
	CC1_1	MultipleChoiceQuestion					Text	1.Idiegti automatizuotus inventoriaus (tinkle mazgu) aptikimo irankius.	YesNoValuesList				
								Reikalingi tiek aktyvus irankiai,					
								2. Idiegti DHCP serverio zurnala ir					
								taip pageriniti tinklo mazgu					
	CC1_2	MultipleChoiceQuestion					Text	inventorizacija bei palengvinti	YesNoValuesList				
								nezinomu sistemu aptikima.					
	CC1_3	MultipleChoiceQuestion					Text	3.Visa naujai prie tinklo prijungta iranga turetu buti autom	YesNoValuesList				
								4. Palaikyti tinklo ir prijungtu mazgu					
	CC1_4	MultipleChoiceQuestion					Text	inventoriu, kuriame turetu buti	YesNoValuesList				
								matomi: IP adresai, mazgo					
	CC1_5	MultipleChoiceQuestion					Text	5. Butina dargti ir saugioje vietoje	YesNoValuesList				
								saugoti inventoriaus kopijas.					
	CC1_6	MultipleChoiceQuestion					Text	6. Reikia sudaryti kritines	YesNoValuesList				
								informacijos sarasa, nurodant, kur ji					
	CC1_7	MultipleChoiceQuestion					Text	7. Panaudokite 802.1x protokola irenginiu prisijungimo pi	YesNoValuesList				
								##########					
	CC1_8	MultipleChoiceQuestion					Text		YesNoValuesList				
	CC1_9	MultipleChoiceQuestion					Text	9. Sukurkite atskira VLAN BYOD (angl. Bring your own d	YesNoValuesList				
	CC1_10	MultipleChoiceQuestion					Text	10. Panaudokite klientu sertifikatus, kad patikrintumete ji	YesNoValuesList				
	IMP1	Impact	CC1_1	answer	is	Taip	Text						&automatizuokite invento
	IMP2	Impact	CC1_2	answer	is	Taip	Text						Įdiekite DHCP zumaliza

Taisyklių įvedimo darbolapis

Priedas Nr.2

Kitų maršrutizatorių konfiguracija analogiška

```
!

!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 debugging
!
username viliusp privilege 15 password 7 00071A150754
no aaa new-model
ip subnet-zero
!
!
!
!
no ip domain lookup
ip domain name test.ktu.lt
ip ssh break-string
ip ssh version 2
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
!
!
!
no crypto isakmp enable
!
!
!
interface FastEthernet0/0
description R2 f0/0
ip address 172.16.0.1 255.255.255.252
speed 100
full-duplex
!
interface FastEthernet0/1
description NMAP GW
ip address 192.168.0.254 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet1/0
```

```
description VMware GW
ip address 192.168.242.254 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet2/0
description R5(FW) f2/0
ip address 10.1.0.1 255.255.255.252
duplex auto
speed auto
!
router eigrp 1
redistribute connected
passive-interface FastEthernet0/1
passive-interface FastEthernet1/0
network 172.16.0.0
network 192.168.0.0
network 192.168.242.0
auto-summary
ip classless
no ip http server
no ip http secure-server
control-plane
line con 0
exec-timeout 0 0
privilege level 15
password 7 0822455D0A16
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
privilege level 15
login local
transport input ssh
!
!
end
```

Priedas Nr.3

OVAL rezultatų failo skaitymas

```
NodeList definition_list = doc.getElementsByTagName("oval-def:definition");
for (int temp = 0; temp < definition_list.getLength(); temp++) {

	String id = null;
	Node nTitle = null;;
	Node nDescription = null;
	Node nCriteria = null;
	Node nMeta = null;
	Node nReference = null;



	Node nDefinition = definition_list.item(temp);		// Aprašų sąrašas
	NodeList def_child_list = nDefinition.getChildNodes();
	if (nDefinition.getNodeType() == Node.ELEMENT_NODE  )  {
		Element eDefinition = (Element) nDefinition;
		id = eDefinition.getAttribute("id");
	}


	for (int temp2 = 0; temp2 < def_child_list.getLength(); temp2++){
		if (def_child_list.item(temp2).getNodeName() == "oval-def:metadata"){
			nMeta = def_child_list.item(temp2);
		}
		if (def_child_list.item(temp2).getNodeName() == "oval-def:criteria"){
			nCriteria = def_child_list.item(temp2);
		}
	}


	NodeList criteria_list = nCriteria.getChildNodes();  // Krit. sub-mazgai
	NodeList meta_list = nMeta.getChildNodes();          // Meta sub-mazgai



	for (int temp3 = 0; temp3 < meta_list.getLength(); temp3++){
		if (meta_list.item(temp3).getNodeName() == "oval-def:title"){
				nTitle = meta_list.item(temp3);
		}
		if (meta_list.item(temp3).getNodeName() == "oval-def:description"){
			nDescription = meta_list.item(temp3);
		}
		if (meta_list.item(temp3).getNodeName() == "oval-def:reference"){
			nReference = meta_list.item(temp3);
		}
	}

	String vulnTitle = nTitle.getTextContent();
	String vulnDesc = nTitle.getTextContent();
	Element eVulnRef = (Element) nReference;
	String vulnRef = eVulnRef.getAttribute("ref_id");
	for (int temp5 = 0; temp5 < def_child_list.getLength(); temp5++){
		if (matching_def[temp5].equals(vulnRef)){
			pw.println(vulnRef);
		}
	}
```