****

**Kauno technologijos universitetas**

Informatikos fakultetas

**Ugniasienių (užkardų) tipai ir apėjimo metodika**

Referatas

|  |
| --- |
|  |
| **Eligijus Kiudys**  Projekto autorius |
|  |
|  |
|  |

**Kaunas, 2021**

Turinys

[Lentelių sąrašas (pagal poreikį) 3](#_Toc87440816)

[Paveikslų sąrašas (pagal poreikį) 4](#_Toc87440817)

[Įvadas 5](#_Toc87440818)

[Analizė 6](#_Toc87440819)

[Ugnesienių metodologijos apėjimo aptikimas 7](#_Toc87440820)

[Apibendrinimas ir išvados 8](#_Toc87440821)

[2. Skyriaus pavadinimas 9](#_Toc87440822)

[3. Skyriaus pavadinimas 13](#_Toc87440823)

[4. Skyriaus pavadinimas 15](#_Toc87440824)

[Išvados 16](#_Toc87440825)

[Literatūros sąrašas 17](#_Toc87440826)

Lentelių sąrašas (pagal poreikį)

[**1 lentelė.** Pagrindiniai baigiamojo projekto stiliai ir jų aprašymai 6](#_Toc87342002)

Paveikslų sąrašas (pagal poreikį)

[**1 pav.** Kauno technologijos universiteto „Santakos“ slėnio fasadas 10](#_Toc87342005)

Įvadas

Ugniasienes – yra specialus filtras, kuri filtruoja ateinančia ir išeinančia informaciją, kurią leidžia išsiūti arba priimti įrenginyje, taip saugo įrenginį nuo įvairių atakų. Dažniausiai ugniasienės yra programinės arba fizinės. Programinės ugniasienės yra naudojamos vieno įrenginio informacijai tinkle reguliuoti. Fizinės ugniasienės yra naudojamos lokalaus tinklo informacijos valdymui. Tokios ugniasienės dažniausiai randamos maršrutizatoriuose. Ugniasienių yra skirtingų tipų, pagal ugniasienių tipus, ugniasienės funkcionalumas ir paskirtis pasikeičia. Ugniasienės neužtenka apsisaugoti nuo visų grėsmių, kurios gali grėsti įrenginiui.

Šio darbo tikslas – išanalizuoti ugniasienių tipus ir pasitaikančias apėjimo metodologijas. Darbo uždaviniai:

* Išanalizuoti esamus ugniasienių tipus
* Išanalizuoti pasitaikančias apėjimo metodologijas
* Ugniasienių apėjimo metodologijos aptikimas ir stabdymas

Dokumentą sudaro du pagrindiai skyriai – ugniasienių analizės, apėjimo metodologijų aptikimas ir stabdymas. Ugniasienių analzės skyriuje yra susipažystama su įvairiais ugniasienių tipais. Apžveligiama dažniausiai pasitaikantčias ugnesienių apėjimo metodologijos. Ugnesienių metodologijos apėjimo aptikimo ir stabdymo skyriuje analizuojame kokios yra dažniausiai pasitaikančios ugnesienių apėjimo metodologijos ir kaip jas reikėtų sustabdyti. Pabaigoje yra pateikiamas literatųros sąrašas, kuriuo buvo remtasi rašant šį drabą.

Analizė

## Ugniasienių tipai

Mini ivadas

### Packet-filtering firewalls

Pirmasis yra paprasčiausias ugniasienės tipas yra plačiai naudojamas paketų filtras. Naudojamas filtras valdo paketus arba duomenų perdavimą, praleidžiant arba sunaikinat paketą arba neleidžia pasiekti duomenų srautui siuntėjo, pagal tam tikrus standartus:

* Adresas iš kur paketas yra siunčiamas
* Adresas kur paketas yra siunčiamas
* Aplikacijos protokolai arba taisyklės kurios yra skirtos duomenų praleidimui.

Paketus filtruojanti ugniasiene pirmiausia analizuoja paketų siuntėjo, ir gavėjo adresus, portus ir protokolus (pav. 1). Ugniasienes tikrina pagal analizuojamus kriterijus ir nusprendžia ar priimti paketą ar jį numesti pagal ugniasienes naudojamas taisykles.

**Diagram

Description automatically generated**

pav. 1 Paprastos ugniasienes veikimo schema

### Application-level gateways firewalls (a.k.a. proxy firewalls)

Užkarda, kuri pašalina tiesioginį ryšį tarp įgalioto kliento ir išorinio kompiuterio, filtruojant visus gaunamus ir siunčiamus paketus OSI modelio taikymo sluoksnyje. Visi paketai kurie yra išsiunčiami ir priimami vyksta per aplikaciją kuri simuliuoja vidinį serverį, arba per egzistuojantį serverį. Kadangi visas srautas vyksta per serverį ar tai butu lokalus ar realus, jame yra stebimas užklausų duomenų srautas. Tarp kompiuterio ir serverio yra sukuriama sesija kuria yra komunikuojama tarpusavyje. Naudotojas norėdamas prisijungti prie puslapio siunčia užklausą į serverį, kuris siunčia užklausą į internetą. Iš interneto užklausos rezultatai yra gražinami į serverį. Šis serveris nusprendžia ar užklausa turi pasiekti užklausos savininką (pav. 2).

**Diagram

Description automatically generated**

pav. 2 Proxy ugniasiene

### Next-generation firewall (NGFW)

Naujos kartos ugniasiene yra patobulinta ugniasiene, kuri apima tradicinės ugniasienės funkcijas ir turi naujų funkcijų kurios padeda aptikti ne tik tinklo atakas, bet ir aplikacijų atakas. Naujos kartos ugniasienė gali aptikti ir blokuoti aplikacijas, ši ugniasienė pastoviai tikrina tinklą ir bando aptikti bandymą įsilaužti į kompiuterį (IPS). Ši ugniasienė taip pat atlieka URL filtravimą, kuris neleidžia pasiekti puslapių kurie gali būti kenksmingi, taip apsaugant naudotoją nuo vidinių atakų. Kadangi ugniasienė pastoviai tikrina tinklą ir naudojamą kompiuterį, ji gali labai greitai aptikti kenkėjiškas programas arba duomenis ir juos sustabdyti. Šios ugniasienės veikimas išlieka tas pats kaip ir tradicinės ugniasienės, bet su nauju funkcionalumu, kuris padeda apsaugoti naudotoją dar labiau. Į naujos kartos ugniasienes dažniausiai įeina tokios funkcijos kaip: VPT (angl. VPN), antivirusinė, URL filtravimas, smėlio dėžė, SSL patikrinimas, apsaugos sistema skirta apsisaugoti nuo įsibrovimų.

### Stateful Inspection (Busenos ugniasiene )

Dažniausia būsenos tipo ugniasienės yra saugesnė nei paprasta paketų filtravimo ugniasienė. Ši ugniasienė seka duomenų srautą ir būsenas, ne veltui ši ugniasienė yra pavadinta būsenos ugniasienė. Jei reikėtu tiksliau paaiškinti tai būtų, kad naudotojo kompiuteriui siunčiant užklausą per ugniasienę, ji seka paketą. Gavus rezultatą ir interneto yra patikrinamas ar paketo siuntėjas naudotojui atitinka naudotojo kompiuterio išsiustam siuntėjui. Kitas dalykas kurį naudoja šio tipo ugniasienė tai yra, kad pagal būseną galima dinamiškai atidaryti arba uždaryti prievadu, gali pridėti dinamiškai taisykles pagal kurias veiki ugniasienė.

### Circuit-level gateway ()

Tai tokia ugniasienė, kuri seka ir tvirtina TCP protokolą. Ši ugniasienė tikrina, ar galima sukurti sesiją tarp dviejų įrenginių. Ugniasienės duomenų srautas yra valomas pagal tai ar prašoma sesija yra tikra. Į sesijos tikrinimą įeina: patikrinama ar naudotojo užklausa valdi, yra naudojami paprasti filtravimo kriterijai kaip naudotojo IP adresas, TCP protokolo sudėtis. Filtruojant užklausą ji gali būti atmesta arba patvirtina, taip yra atfiltruojamos tinklo užklausos.

## Pasitaikančios apėjimo metodologijos

Mini ivadas

### Insider Attacks

Tai dadžiausiai tokia ataka kuri vyksta iš vidaus. Tokią ataką dažniausiai įvyksta tai, kažkoks žmogus bando pakenkti organizacijai iš vidaus. Tai gali būti darbininkas, kuris turi priėjima prie organizacijos tinklo. Gali būti darbininkas, kuris nežinant paplatina duomenis, arba leidžia prisijungti kitiems asmenism. Gali būti, įsilauželis kuris apsimeta kompanijos darbuotoju, kitaip sakant žmogus kuris nedriba organizacijoje bet vis tiek gauna, kažkokiais būdais organizacijos privilegijas, trumpiau sakant apgavikas. Būna tokių situacijų, kad darbuotojas atsidaro elektroninį laišką, kurio palgaba įsilauželis gali prisijungti prie organizacijos tinklo.



pav. 3 Kompanijų savininkų ir rangovų apklausa ([Top Insider Threat Concern? Careless Users. [Survey] | Imperva](https://www.imperva.com/blog/top-insider-threat-concern-careless-users-survey/))

Buvo padaryta apklausa apie vidinias atakas. Žonės buvo klausinėjami kokių atakų labiausiai bijo.

Daugiausiai bijo nesaugaus darbuotojo, kuris gali nežinodamas paskleisti kompanijos jautrius duomenis. Compromituoti naudotojai, kurie pametė savo duomenis, arba jų duomenys buvo nulaudžti surinko panašų procentų kiekį kaip ir naudotojai, kurie specialiai laužiasi į organizacjijos tinklą, naudotojai kurie vagia duomenis arba specialiai naikina sistemas.

### Missed Security Patches

Šita problema egzistuoja ne vien ugnesienėje, bet ir progamose, operacinėse sistemose. Pirmiausia reikia suprasti, kas yra saugos pataisa. Tai saugos pataisa yra, aptikus kažkokią saugos spragą programoje ar kitokioje vietoje ji yra pataisoma ir atnaujinama visiems naudotojamas. Saugos pataisa padeda apsaugoti naudotojo programinę įrangą nuo skylių kuriomis gali pasinaudoti įsilauželiai. Neatnaujinama prgigraminė įranga gali būti nesaugi, kadangi atsiranda naujų pažeidimų kuriais įsilauželiai gali pasinaudoti. Dažniausiai atradus tokią skylė programinės įrangos kūrėjai bando sutvarkyti esamą skylę kuo greičiau, bet skylės sutvarkymas gali užtrukti. Per laiką kurį yra tvarkoma nauja spraga, įsilaužėliai gali ja pasinaudoti ir atlikti labai daug žalos.

### Configuration Mistakes ([Five Firewall Configuration Mistakes You Need to Avoid | IT Infrastructure Advice, Discussion, Community - Network Computing](https://www.networkcomputing.com/network-security/five-firewall-configuration-mistakes-you-need-avoid))

Ugnesienės blogos konfiguracijos klaidos pasitaiko dažnai. Net jei ir ugniasienė yra suknofiguruota ji gali būti neveiksimnga, arba tik dalinai veiksminga. Dažniausiai yra penkios problemos ugniasienės konfiguravime.

1. Blogai sukonfiguruota ugniasienė kuri yra skirta debesų struktūrai

Viena iš didžiausių problemų šioje srityje yra, tinklo pasiekimas iš bet kokios vietos. Kadangi naudojant debesų technologiją, aplikacijoms kurios naudoja debesų technologiją reikia pasiekimo iš bet kur. Tokių būdu sukonfigūruotas ugniasienes galima įsilaužti, kadangi turi būti atvira prieiga, kuri leistų įvairioms programoms bei naudotojams užtikrinti prieigą iš bet kurios vietos.

1. Blogai sukonfigūruotos prievado taisyklės

Tokia klaida dažniausiai yra padaroma, dėl prievado konfigūracijos lengvumo. Konfigūruojant prievadą ugniasienėje dažniausiai yra neapribojamas tinklo pasiekimas per prievadą. Tokiu konfigūravimo būdu kiekvienas naudotojas ar įsilaužėlis gali pasiekti tinklą per atidarytą privedą.

1. Ugniasienės naudojimo pradžioje leidimas visiems prieiti

Šita problema rišasi su kitomis minėtomis problemomis. Dažniausiai priėjimas prie norimo nuotolinio tinklo yra sukonfigūruotas taip, kad prie nuotolinio tinklo gali prieiti visi. Laikui einant yra pridedamos naujos taisyklės, kurios pradeda riboti lokalaus tinklo priėjimą prie kito tinklo. Žinoma taip gali ir neįvykti. Laiko tarpui, kai tinklą gali prieiti, bet kas įsilaužėliai gali pasinaudoti šiuo laiko tarpu ir padaryti daug žalos.

1. Nesukonfigūruotas išėjimo filtras

Dažniausiai ugniasienės nėra filtruojamas išėjimo filtravimas. Naudotojas gali išsiūti bet kokią užklausą kur tik nori. Tai leidžia naudotojui lankytis nesaugiuose puslapiuose, ar tai leidžia parsisiųsti virusus, apie kuriuos gali pats naudotojas nežinoti.

1. Tikint, kad gerai sukonfigūruotos ugniasienės užtenka apsisaugoti nuo tinklo atakų

Sukonfigūravus ugniasienę tvarkingai, peržiūrėjus visas taisykles, neleidžiant visiems prisijukti prie tinklo ir kitaip apribojant tinklo pasiekiamumo. Tai nereiškia, kad naudotojas ar tinklas yra apsaugotas. Yra įvairių įsibrovimo būdų, nebūtinai galima įsibrauti tiesiogiai per ugniasienę.

### DoS ir DDoS ataka

DDoS arba DoS atakos yra skirtos, stabdyti tinklo veikimą. Tokios atakos yra vykdomos labai dažnai, kadangi jos yra labai paprastos. Tokios atakos yra paremtos tinklo užpildymu, įsilaužėliai siunčia kiek gali daugiau paketų į atakuojamą tinklą, taip jį prilėtinant arba sustabdant. Kadangi tokia ataka daug resursų nenaudoja ji yra populiari ir efektyvi. Ugniasienės gali šiek tiek valdyti tokias atakas, priklauso nuo atakos dydžio. Jei ataka yra labai didelė, skaičiais sunku pasakyti, kadangi gali labai keistis priklausant nuo naudojamos ugniasienės, bei interneto greičio, jos vis tiek gali savo kiekiu užversti ugniasienę paketais taip stabdant tinklą (pav. 4).

Diagram

Description automatically generated

pav. 4 DoS ir DDoS

### Social engineering

Socialinė inžinerijos ataka yra labiausiai paplitusi internete. Šitame spektre yra ne viena ir ne dvi atakos. Socialinė inžinerija yra tokios atakos kurios yra kompiuterio naudotojui. Tokios atakos gali remtis naudotojo jausmais, bandant apgauti naudotoją, ar bandant išgauti kažkokią informaciją, kuri dažniausiai būna slaptažodžiai, ar kita informacija kuria būtų galima pasinaudoti.

### ****Baiting****

Viena iš populiariausių esamų atakų yra gundymas (angl. baiting). Tokios atakos dažniausiai kažką siūlo, kaip nemokamos muzikos parsisiuntimą, nemokamų kodų parsisiuntimą ir t.t. Šita programa kažką siūlo kuom naudotojas galėtų susigundyti. Dažniausiai paspaudus ant parsisiuntimo mygtuko tokių atakų metu yra prašoma įvesti asmeninius duomenis, užpildyti pateiktą formą, kad būtų galima kažką atsisiųsti ar gauti. Tačiau nebūtinai tokios atakos gali būti internetinės, tokios atakos gali vykti ir fiziškai. Gali būti atsiunčiamas usb įrenginys kuris turi virusą.

### ****Scareware****

Dažniausiai ši ataka yra skirta įbauginti naudotoją ar jį įtikinti, kad jų kompiuteryje yra kažkoks tai virusas, kuris gali neegzistuoti. Naudotoją įtikinus, yra siūloma parsisiųsti netikrą antivirusinę kuri gali ištrinti netikra virusą, tokios antivirusinės dažniausiai būna kažkokio tipo virusas.

### ****Pretexting****

Vienas iš pavyzdžių būtų siurprizo planavimas. Apgavikas dažniausiai bando naudoti žodžius kurie tiktų kiekvienam. Apgavikas prašo nupirkti svarbų pirkinį, komandos siurprizui.

### ****Phishing****

Dažniausia ataka internete. Tokios atakos pasitaiko kiekvieną dieną. Dažniausiai yra atsiunčiamas elektroninis laiškas prašant atnaujinti slaptažodį ar atnaujinti kitą informaciją (pav. 5). Gali būti ir reklamų kurios siūlo nusipirkit brangų daiktą su didele akcija. Dažniausiai paspaudus ant duotos nuorodos elektroniniame laiške yra pateikiama realaus puslapio kopija, arba netikras puslapis kuris atrodo realiai. Prisijungus į puslapio kopiją dažniausiai įvesti duomenys yra pasisavinami ir netikras puslapis nukreipia naudotoją į tikrą puslapį. Netikri puslapiai kurie parduoda daiktus, tiesiog pasisavina pinigus ir neina jų susekti.

**Graphical user interface, text, application, email

Description automatically generated**

pav. 5 Phishing atakos pavyzdys

### ****Spear phishing****

Dažniausiai tokios atakos yra suasmenintos. Apgavimas bando suprasti kuo daugiau apie auką, kad galėtų parašyti kuo asmeniškesnį laišką, kuriuo auka galėtų patikėti. Tokios atakos dažniausiai bando gauti naudotojo informaciją kaip slaptažodžiai, banko informacija ir t.t. Dažniausiai būna išsiunčiamas elektroninis laiškas aukai su prisegtu failu. Elektroniniame laiške dažniausiai yra rašoma, kad informacijos reikia labai greitai. Apgavikai apsimeta kaip draugais ir prašo tokios informacijos kaip socialinių tinklų prisijungimo informacijos.

Ugnesienių metodologijos apėjimo aptikimas ir stabdymas

## Insider Attacks

Tokio tipo ataką nėra labai lengva aptikti. Kadangi dažniausiai tokios atakos įvykstą per darbininką, galima tokių atakų išvengti apribojus interneto prieigą. Prieigos apribojimas nėra idealus sprendimas, bet jie vienas iš galimų. Dažniausiai didelėse įmonėse yra atsakingi darbuotojai kurie stebi tinklo veiklą ir ieško anomalijų kurios galėtų parodyti vidinę ataką. Žinoma yra sukurta ir programinė įranga kuri gali stebėti tinklo ar kompiuterių anomalijas, bet geriausias pasisaugojimo būdas yra turėti asmenį kuris yra už tai atsakingas ir ieško aktyviai naujų ir senų problemų.

## Missed Security Patches

Ši problema yra lengviausiai išsprendžiama, kadangi reikia atnaujinti programinę įrangą. Žinoma yra programinės įrangos dalis kuri atsinaujina automatiškai, bet yra ir tokių programinių įrangų kurias reikia atnaujinti rankinių būdu. Reikėtų stengtis tikrinti programinės įrangos atnaujinimus kuo dažniau, kadangi atsiranda naujų sutvarkymų ir užlopytų saugos skylių.

## Configuration Mistakes

## DDoS ataka

## Social engineering

Apibendrinimas ir išvados

# Skyriaus pavadinimas

Lorem ipsum dolor sit amet, eam ex decore persequeris, sit at illud lobortis atomorum. Sed dolorem quaerendum ne, prompta instructior ne pri. Et mel partiendo suscipiantur, docendi abhorreant ea sit. Recteque imperdiet eum te.

Eu eum decore inimicus consetetur, cu usu habeo corpora intellegam. Ut antiopam efficiendi deterruisset sit. Mel sint eirmod id, qui quot virtute id, dolor nemore forensibus usu id. Fugit dolore voluptatum cu vim. An vix veniam graecis insolens, sit posse iusto id. Ut vim ceteros percipit, id quo ubique recusabo, eum sint lucilius ea. In sumo inani numquam has.

## Poskyrio pavadinimas

Lorem ipsum dolor sit amet, eam ex decore persequeris, sit at illud lobortis atomorum. Sed dolorem quaerendum ne, prompta instructior ne pri. Et mel partiendo suscipiantur, docendi abhorreant ea sit. Recteque imperdiet eum te.



**6 pav.** Kauno technologijos universiteto „Santakos“ slėnio fasadas

Literatūros sąrašas

1. Literatūros šaltinis
2. Literatūros šaltinis
3. Literatūros šaltinis
4. Literatūros šaltinis