****

**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

Pirmasis yra paprasčiausias ugniasienės tipasir plačiai naudojamas paketų filtras. Įrengta dviem tinklo sąsajos kortelėmis (NIC) ir funkcijomis filtruoti (filtruoti) įvairius gaunamus paketus. Paketų filtras dar vadinamas paketo filtravimo maršrutizatoriumi.

**Diagram

Description automatically generated**

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

programos lygio šliuzas

Užkarda, kuri pašalina tiesioginį ryšį tarp įgalioto kliento ir išorinio kompiuterio, filtruojant visus gaunamus ir siunčiamus paketus OSI modelio taikymo sluoksnyje.

### Next-generation firewall (NGFW)

Naujos kartos ugniasienės apima tris funkcijas: ugniasienę, IPS ir aplikacijų kontrolę. NGFW suteikia papildomą kontekstą ugniasienės sprendimų priėjimui, tikrina srautą (DPI) ir įžvelgus rizikas – jį blokuoja.

Yra daug skirtingu implementaciju

Naujos kartos ugniasienės apjungia tradicines funkcijas – paketų filtravimą, NAT, URL filtravimą, VPN su Qos. Bei naujas – IPS, SSL ir SSH patikra, DPI, reputacija pagrįstu kenkėjiškos programinės įrangos aptikimą, aplikacijų kontrolę. Tai atsakas į didėjančias grėsmes L4-L7 lygyje.

### Stateful Inspection

Dažniausias perimetro užkardos tipas yra valstybinis tikrinimo užkarda. Valstybinė patikrinimo užkarda saugo visą išeinančio tinklo srautą ir leidžia tik įeinantį srautą, turintį atitinkamą užklausą. Valstybinės tikrinimo užkardos gali užblokuoti nuskaitymą iš interneto ir užkirsti kelią IP spoofingui - kai užpuolikas gauna neteisėtą prieigą prie tinklo ar kompiuterio, įvardydamas savo interneto protokolo (IP) adresą. Valstybinės tikrinimo užkardos tikrina daugiau duomenų nei statiniai paketų filtro užkardos ir atitinkamai mažesni.

### Circuit-level gateway

grandinės lygio šliuzas

Užkarda, kuri neleidžia tiesiogiai bendrauti tarp įgalioto kliento ir išorinio kompiuterio. Pirmiausia ji priima patikimo kliento užklausą dėl tam tikrų paslaugų ir, patikrinusi, ar prašoma sesija galioja, užmezga ryšį su išoriniu priegloba.

## Pasitaikančios apėjimo metodologijos

Mini ivadas

### Insider Attacks

Insider threats can be harder to identify or prevent than outside attacks, and they are invisible to traditional security solutions like firewalls and intrusion detection systems, which focus on external threats. If an attacker exploits an authorized login, the security mechanisms in place may not identify the abnormal behavior. Moreover, malicious insiders can more easily avoid detection if they are familiar with the security measures of an organization

### Missed Security Patches

This is an issue that arises when network firewall software isn’t managed properly. For any software program, there are vulnerabilities that attackers may exploit—this is as true of firewall programs as it is of any other piece of software. When firewall vendors discover these vulnerabilities, they usually work to create a patch that fixes the problem as soon as possible.

However, the patch’s mere existence doesn’t mean that it will automatically be applied to your company’s firewall program. Until that patch is actually applied to your firewall software, the vulnerability is still there—just waiting to be exploited by a random attacker.

The best fix for this problem is to create and stick to a strict patch management schedule. Under such a schedule, you (or the person managing your cybersecurity) should check for any and all security updates for your firewall software and make sure to apply them as soon as possible.

### Configuration Mistakes

Even when a firewall is in place on your network, and has all of the latest vulnerability patches, it can still cause problems if the firewall’s configuration settings create conflicts. This can lead to a loss of performance on your company’s network in some cases, and a firewall outright failing to provide protection in others.

For example, dynamic routing is a setting that was long ago deemed a bad idea to enable because it results in a loss of control that reduces security. Yet, some companies leave it on, creating a vulnerability in their firewall protection.

Having a poorly-configured firewall is kind of like filling a castle’s moat with sand and putting the key to the main gate in a hide-a-key right next to the entrance—you’re just making things easier for attackers while wasting time, money, and effort on your “security” measure.

### A Lack of Deep Packet Inspection

Layer 7 (or “deep packet”) inspection is a rigorous inspection mode used by next-generation firewalls to examine the contents of an information packet prior to approving or denying that packet passage to or from a system.

Less advanced firewalls may simply check the data packet’s point of origin and destination before approving or denying a request—info that an attacker can easily spoof to trick your network’s firewall.

The best fix for this problem is to use a firewall that can perform deep packet inspection to check information packets for known malware so it can be rejected.

### DDoS Attacks

Distributed Denial of Service (DDoS) attacks are a frequently-used attack strategy noted for being highly effective and relatively low-cost to execute. The basic goal is to overwhelm a defender’s resources and cause a shutdown or prolonged inability to deliver services. One category of attack—protocol attacks—are designed to drain firewall and load balancer resources to keep them from processing legitimate traffic.

While firewalls can mitigate some types of DDoS attacks, they can still be overloaded by protocol attacks.

There is no easy fix for DDoS attacks, as there are numerous attack strategies that can leverage different weaknesses in your company’s network architecture. Some cybersecurity service providers offer “scrubbing” services, wherein they divert incoming traffic away from your network and sort out the legitimate access attempts from the DDoS traffic. This legitimate traffic is then sent to your network so you can resume normal operations.

### Social engineering

Social engineering refers to a wide range of attacks that leverage human interaction and emotions to manipulate the target. During the attack, the victim is fooled into giving away sensitive information or compromising security.

A social engineering attack typically takes multiple steps. The attacker will research the potential victim, gathering information about them and how they can use them to bypass security protocols or get information. Then the attacker does something to gain the target’s trust before finally manipulating them into divulging sensitive information or violating security policies.

Ugnesienių metodologijos apėjimo aptikimas ir stabdymas

Apibendrinimas ir išvados

## 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.

**1 lentelė.** Pagrindiniai baigiamojo projekto stiliai ir jų aprašymai

| **Stiliaus pavadinimas** | Stiliaus pavadinimas galerijoje | Stiliaus formalieji reikalavimai | Stiliaus naudojimo aprašymas |
| --- | --- | --- | --- |
| Antraštė non-TOC | Antraštė non-TOC | Šrifto dydis 12 pt, šriftas paryškintas, intervalas tarp eilučių – 1,15, atstumas prieš ir po antraštės – 10 pt, centruota lygiuotė. | Antraštėms, kurios nėra įtraukiamos į turinį: „Santrauka“, „Summary“, „Turinys“. |
| Antraštė be nr. | Antraštė be nr. | Šrifto dydis 12 pt, šriftas paryškintas, intervalas tarp eilučių – 1,15, atstumas prieš ir po antraštės – 10 pt, centruota lygiuotė, antraštė rašoma naujame puslapyje – po puslapio skirtuko. | Antraštėms, kurios įtraukiamos į turinį, bet nėra numeruojamos: „Lentelių sąrašas“, „Paveikslų sąrašas“, „Santrumpų ir terminų sąrašas“, „Įvadas“, „Išvados“, „Literatūros sąrašas“, „Informacijos šaltinių sąrašas“, „Priedai“. |
| 1. Heading 1,Skyrius | Skyrius | Šrifto dydis 12 pt, šriftas paryškintas, intervalas tarp eilučių – 1,15, atstumas po antraštės – 10 pt, abipusė lygiuotė, antraštė rašoma naujame puslapyje – po puslapio skirtuko. | Skyrių antraštėms, kurios įtraukiamos į turinį ir yra numeruojamos. |
| 1.1. Heading 2,Poskyris | Poskyris | Šrifto dydis 12 pt, šriftas paryškintas, intervalas tarp eilučių – 1,15, atstumas prieš ir po antraštės – 10 pt, abipusė lygiuotė, numeracija siejama su aukštesnio lygio antrašte. | Poskyrių antraštėms, kurios įtraukiamos į turinį ir yra numeruojamos. |
| 1.1.1. Heading 4,Skyrelis | Skyrelis | Skyrelių antraštėms, kurios įtraukiamos į turinį ir yra numeruojamos. |
| Tekstas | Tekstas | Šrifto dydis 12 pt, intervalas tarp eilučių – 1,15, atstumas prieš pastraipą – 10 pt, abipusė lygiuotė. | Tekstui visose projekto dalyse (santraukose, įvade, skyriuose, poskyriuose ir t.t.). |
| List Bullet;Sąrašas (suženklintas) | Sąrašas (suženklintas) | Pirmos pastraipos eilutės įtrauka – 0,63 cm, šrifto dydis 12 pt, intervalas tarp eilučių – 1,15, atstumas tarp tokio paties stiliaus pastraipų – 0 pt, atstumas po sąrašo – 10 pt, abipusė lygiuotė. | Tekstui, kuris pateikiamas suženklintu sąrašu. |
| List Number;Sąrašas (numeruotas) | Sąrašas (numeruotas) | Šrifto dydis 12 pt, intervalas tarp eilučių – 1,15, atstumas tarp tokio paties stiliaus pastraipų – 0 pt, atstumas po sąrašo – 10 pt, abipusė lygiuotė. | Tekstui, kuris pateikiamas sunumeruotu sąrašu. |
| Footnote Text;Išnašos tekstas | Išnašos tekstas | Šrifto dydis 10 pt, intervalas tarp eilučių – 1,15, atstumas prieš ir po sąrašo – 0 pt, abipusė lygiuotė. | Tekstui, kuris pateikiamas išnašose. |
| Lentelės pavad. | Lentelės pavad. | Šrifto dydis 11 pt, intervalas tarp eilučių – 1,15, atstumas prieš pavadinimą – 10 pt, po pavadinimo – 3 pt, lygiuotė prie kairiojo krašto. | Lentelių pavadinimams (numeris ir žodis lentelė rašomas paryškintu šriftu). |
| Lentelės I eil. | Lentelės I eil. | Šrifto dydis 10 pt, šriftas paryškintas, intervalas tarp eilučių – 1,15, atstumas prieš ir po pastraipos – 3 pt, lygiuotė prie kairiojo krašto. | Tekstui lentelės antraštinei (pirmai) eilutei. |
| Lentelė | Lentelė | Šrifto dydis 10 pt, intervalas tarp eilučių – 1, atstumas prieš ir po pastraipos – 3 pt, lygiuotė prie kairiojo krašto. | Tekstui lentelėje. |
| Caption,Paveikslo pavad. | Paveikslo pavad. | Šrifto dydis 11 pt, intervalas tarp eilučių – 1,15, atstumas prieš ir po pavadinimo – 10 pt, centruota lygiuotė. | Paveikslų pavadinimams (numeris ir santrumpa pav. rašoma paryškintu šriftu). |
| Figure;Paveikslas | Paveikslas | Atstumas prieš ir po paveikslo – 10 pt, centruota lygiuotė. | Paveikslui, iliustracijai . |
| Bibliography,Bibliografija | Bibliografija | Šrifto dydis 12 pt, intervalas tarp eilučių – 1,15, atstumas tarp tokio paties stiliaus pastraipų – 2 pt, abipusė lygiuotė. | Literatūros ir Informacijos šaltinių sąrašuose nurodytiems šaltiniams. |
| Priedas | Priedas | Šrifto dydis 12 pt, šriftas paryškintas, intervalas tarp eilučių – 1,15, atstumas prieš ir po antraštės – 10 pt, lygiuotė prie kairiojo krašto. | Priedo numeriui, žodžiui *priedas*, priedo pavadinimui. |
| TOC 1,Turinys 1 | Turinys 1 | Šrifto dydis 12 pt, šriftas paryškintas, intervalas tarp eilučių – 1,15, įtrauka – 0,64. | Turinyje esančioms antraštėms, kurios nėra numeruojamos („Lentelių sąrašas“, „Paveikslų sąrašas“, „Santrumpų ir terminų sąrašas“, „Įvadas“, „Išvados“, „Literatūros sąrašas“, „Informacijos šaltinių sąrašas“, „Priedai“) ir numeruojamai antraštei „Skyriaus pavadinimas“. |
| TOC 2,Turinys 2 | Turinys 2 | Šrifto dydis 12 pt, intervalas tarp eilučių – 1,15, įtrauka – 0,96. | Turinyje esančiai antraštei „Poskyrio pavadinimas“. |
| TOC 3,Turinys 3 | Turinys 3 | Šrifto dydis 12 pt, intervalas tarp eilučių – 1,15, įtrauka – 1,28. | Turinyje esančiai antraštei „Skyrelio pavadinimas“. |
| TOC 4,Turinys 4 | Turinys 4 | Šrifto dydis 12 pt, intervalas tarp eilučių – 1,15, įtrauka – 0,64. | Numeruotiems priedams. |

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[[1]](#footnote-2).

# 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.



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

Išvados

1. 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.
2. 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.

Literatūros sąrašas

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

1. 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. [↑](#footnote-ref-2)