

VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

ELEKTRONIKOS fakultetas

TELEKOMUNIKACIJŲ INŽINERIJOS katedra

Paulius Putrius

**INFORMACIJOS IR SISTEMŲ APSAUGA**

VLAN Saugumas

Namų darbas

Dėstytojas: Eimantas Garšva

Vilnius, 2018

TURINYS

[ĮVADAS 2](#_Toc509926178)

[VLAN ATAKŲ TIPAI IR SAUGUMAS 3](#_Toc509926179)

[1. Media Access Control (MAC) lentelės perpildymas 3](#_Toc509926180)

[2. Komutatoriaus suklastojimo/ VLAN hopping ataka 3](#_Toc509926181)

[3. Dvigubos inkapsuliacijos VLAN šuolio ataka. 4](#_Toc509926182)

[4. Privačių VLAN (PVLAN) ataka. 4](#_Toc509926183)

[5. Spanning tree protokolo (STP) ataka 5](#_Toc509926184)

[LITERATŪRA 6](#_Toc509926185)

# ĮVADAS

Nuolat augantis kibernetinių nusikaltimų kiekis, nepakankamas žmonių kompiuterinis raštingumas leidžia nežinomiems įsilaužėliams periimti informaciją. Įmonės vis dažniau tampa pagrindiais taikiniais įvairaus masto atakų ir yra priversto vis labiau plėsti ir didinti investicijas į saugumą. Įmonių darbuotojai dažnai nesuvokia galimo pavojaus, rizikos, kuriuos gali sukelti neatsargumas ir aplaidumas. Ir kiekvieną dieną atsiranda naujų grėsmių apie kurias sužinoma dažniausiai jau šiek tiek per vėlai. Todėl kompiuterinių tinklų saugumas yra nuolatos auganti disciplina apimantis vis naujas sritis.

VLAN yra geras sprendimas tvarkant skirtingo saugumo zonų tinklus. Tai tas pats LAN, išskyrus tai, kad naudojant šakotuvų technologijas, skirtingų grupių kompiuteriai tame pačiame tinkle gali būti atvaizduojami skirtinguose tinkluose. Kiekvienas VLAN gali būti suprastas kaip skirtingo saugumo zona. Šios zonos paprastai padeda apsaugoti informacijos vientisumą bei konfidencialumą tarp skirtingų įmonės skyrių (pvz. buhalterija). Šiuo atveju net pasinaudojus tuo pačiu fiziniu kabeliavimu neįmanoma slapta gaudyti tinklo paketų.

Dauguma žmonių kurdami VLAN‘us arba apie juos kalbėdami, dažnai praleidža pagrindinį aspektą dėl kurio jie ir kuria virtualų vietinį tinklą - saugumas . Šiuo metu yra kelios populiariausios atakos, kurios suranda spragas saugumo sistemoje ir jomis pasinaudoja, tai žinoma gali labai pakenkti tiek verslui tiek valstybinės įmonės informacijos nutekinimui. Tokiais atvejais reikia tinkamai suprasti VLAN saugumą ir užkirdti kelią atakoms, arba tinkamai pasiruosšti, kad tos atakos neįvyktų.

Įvykdyti VLAN ataką yra daug paprasčiau nei galima įsivaizuoti. Paprastai net gi galima tiesiog nesunkiai atsiūsti kelias gerai žinomas programas (tokias kaip, *yersinia, dsniff and macof*) ir viskas, jūs turite įrankį ir daug informacijos kaip galite rasti spragas blogai sukonfiguruotame LAN tinkle.

# VLAN ATAKŲ TIPAI IR SAUGUMAS

## Media Access Control (MAC) lentelės perpildymas

MAC ataka yra orientuota į fizinio porto adresus, kuriuose yra aprašyti VLAN parametrai. Dažniausiai MAC lentelės turi aprašytą tam tikrą adresų skaičių pagal nutylėjimą, kas padaro jas pažeidžiamas. Kaip ir buferio perpildymas, šio metodo tikslas yra perpildyti MAC lenteles. Kai lentelė užsipildo komutatorius pradeda persiuntinėti paketus kaip „Hub‘as“ iš kiekvieno porto į visus, atakuojantis žmogus taip pat pradės gauti persiūstus paketus.

Paprasčiausias būdas kaip apsisaugoti nuo šios atakos yra išjungti dabartinį portą ir nustatyti apsaugos prieigą, linus sistemose tai galime padaryti su komanda: **shutdown; switchport mode access, tada panadojus** komandą: **switchport port-security įrašome maksimalų MAC adresų skaičių kuris gali būti įrašytas į MAC lentelę, pvz.: switchport port-security maximum 5. Dabar įvedus komandą switchport port-security violation shutdown, jeigu atakuojantis kompiuteris bandys sugeneruoti daugiau nei 5 MAC adresus portas bus automatiškai išjungtas, taip apsaugant tinklą nuo atakos, taip pat tinklo administratorius gaus „log“ failą apie bandymą įsilaužti su atakuojančio kompiuterio MAC adresu.**

## Komutatoriaus suklastojimo/ VLAN hopping ataka

Šio tipo atakos atsiranda kai komutatorius sąmoningai ir apgaulingai neišsiunčia paketų tarp VLAN‘ų.

Atakos metu atakuojantis kompiuteris imituoja „trunk“ komutatoriu. Tokiu metodu atakuojantis kompiuteris naudojasi DTP (Dynamic Tunking Protocol), tam kad pasiekti VLAN registracijos ir valdymo protokolus, atakuojantis kompiuteris siunčia suklastotas DTP užklausas. VLAN tampa sukompromituotas, tokiu atveju atakuotojas gali įskiepyti į VLAN kitą srautą, kuriuo jis gali gauti jam reikalngą informaciją arba prisijungimo duomenis jeigu jie yra neužšifruoti.

Apsisaugojimui: Pirmiausiai komutatoriuje reikėtų išjungti Dynamic Trunking Protocol, kad portai negalėtų automatiniu būdu pasikeisti į „trunk“ portus (CISCO komutatoriuose tam naudojama komanda: **Switch(config-if)# switchport nonegotiate**), taip pat portai kurie neturėtų išskirtinai būti „trunk“ portai, jie turi būti sukonfiguruoti kaip prieigos portai (CISCO komutatoriuose tam naudojama komanda: **Switch(config-if)# switchport mode access**)

## Dvigubos inkapsuliacijos VLAN šuolio ataka.

Dvigubos inkapsuliacijos ataka galima tik jeigu atkajuontis kompiuteris prijungtas prie sąsajos kuri yra nustatyta kaip vietinis (native) VLAN. Dauguma komutatorių ištrina tik vieną 802.1Q antraštę, šiuo metodu į originalų kadrą yra įrašomos dvi 802.1Q standarto antraštės. Išorinė antraštė priklauso atakuojančio kompiuterio sukurtam VLAN‘ui o kita vidiniam atakuojamo tinklo VLAN‘ui. Kai dvigubos antraštės kadras pasiekia pirmą komutatorių, komutatorius gali matyti tik išorinę antraštę, tuo metu jis ištrina antraštę ir persiunčia ją į visus portus kurie priklauso vietiniam VLAN‘ui. Viena kadro kopija persiunčiama į „trunk“ portą, kad pasiektų antrą komutatorių.

Kai kadras pasiekia antrą komutatorių, atidarydamas kadrą jis matys tik antrą antraštę, todėl pagalvos kad kadras priklauso tam tikram vartotojo VLAN‘ui ir jį persiūs.

Apsisaugojimui, tiesiog laikyti atskirai vietinio (native) VLAN1 trunk portus nuo vartotojo VLAN, pakeičiant vietinius VLAN1 šeimininkus (ang. Hosts) į nenaudojamus VLAN ID, tam naudojama komanda: **Switch(config-if)# switchport access vlan 2 ir Switch(config-if)# switchport trunk native vlan 999,**  kad pakeisti trunk portų VLAN ID.

## Privačių VLAN (PVLAN) ataka.

Privatūs virtualieji tinklai yra išskaidyti į šeimininkų (ang. Hosts) grupes antrajame OSI lygmenyje.

Demilitarizuota zona (DMZ) gali turėti web serverius ir sFTP kurie gali būti pasiekiami iš išorės. PVLAN‘ai yra apsaugoti pagal nutylėjimą antrajame lygmenyje, bet neturi jokios apsaugos trečiajame (tinklo) lygmenyje. Atakuojančiame kompiuteryje sukuriamas kadras su gavėjo maršrutizatoriaus MAC adresu, šaltinio IP adresas gali būti šeimininko (ang. host). Trečiame lygmenyje kadras turi „aukos“ IP adresą, kadangi kadras turi MAC adresą, komutatorius praleidžia kadrą iki maršrutizatoriaus. Maršrutizatorius gavęs kadrą su teisingu IP adresu persiunčia kadrą į „aukos“ kompiuterį. Naudojant šią ataką paketai gali būti tik išsiūsti, kadangi kadrai turės reikiamą IP adresą.

PVLAN atakų galima išvengti naudojant tinkamas ACL (Prieigos kontroliavimo sąrašas) taisykles, kad pagrindiniame LAN tinkle IP adresams būtų uždrausta bendrauti tarpusavyje. Tai reiškia , kad (PVLAN1) gali būti pasiekamas tik tiems serveriams bendraujantiems per komutatorių.

## Spanning tree protokolo (STP) ataka

STP protokolas naudojamas sukurti loginę kilpą Ethernet tinklams. Įrenginiai naudoja BPDU ( Bridge Protocol Data Unit) srautą pasidalinti infromacija tarp įrenginių (STP svarbumo numeris + MAC adresas = BridgeID), kad pasirinkti šakninį tiltą (ang. Root bridge). Tuomet kiekvienas įrenginys pasirenka lengviausią kelią pasiekti „root bridge“ ir nustattyti naudojamą portą.

Įkelės fiktyvų BPDU su suklastotu žemiausiu BDI (Bridge ID), tai padaro įtaką topologijoje ir išrenka atakuojantį kompiuetrį „root bridge“. Tokiu būdu visas srautas yra perimamas atakuojančio kompiuetrio.

Apsisaugojimui nuo tokių atakų reikėtų naudoti tam tikrus nustatymus komutatoriuje:

1. BPDUGuard Enable – nustatymas, kuris naujoma spanning-tree portą padaro erzinančiu, kadangi prieigos įrenginiai negali siųsti BPDU, jeigu BPDU yra gaunamas ant to porto, jis automatiškai yra išjungiamas
2. BPDUFilter – naudojamas BPDU užklausos filtravimui į abi puses. Filtruojami į tinklą patekusios BPDU užklausos. Įjungus šį nustatymą išsijungia STP protokolas, tai gali sukelti kilpas tarp įrenginių.
3. RootGuard – Leidžia įrenginiui dalyvauti STP procese iki tol kol įrenginys nebando gauti root teisių, po bandymo „root guard“ blokuoja portą ir neatblokuoja kol įrenginys baigia siūsti BPDU užklausas.

# LITERATŪRA

<http://www.bluekaizen.org/cam-table-overflow-attack-how-to-prevent-it/>

<https://www.redscan.com/news/ten-top-threats-to-vlan-security/>

<http://www.ciscopress.com/articles/article.asp?p=1681033&seqNum=2>

<https://en.wikipedia.org/wiki/DSniff>

<http://www.blacklabssecurity.info/stp-attacks.html>

<https://en.wikipedia.org/wiki/Bridge_Protocol_Data_Unit>

<https://www.certificationkits.com/cisco-certification/ccna-security-certification-topics/ccna-security-mitigate-layer-2-attacks/ccna-security-preventing-layer-2-attacks/>

<https://en.wikipedia.org/wiki/VLAN_hopping>

<http://www.omnisecu.com/ccna-security/what-is-double-tagging-attack-how-to-prevent-double-tagging-attack.php>

<http://etutorials.org/Networking/Lan+switching+first-step/Chapter+9.+Switching+Security/VLAN-Based+Network+Attacks/>