Kauno technologijos universitetas

Informatikos fakultetas

Ugniasienių (užkardų) tipai ir apėjimo metodika

Referatas

Eligijus Kiudys

Projekto autorius

Kaunas, 2021

Turinys

Paveikslų sąrašas

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 analizės skyriuje yra susipažįstama su įvairiais ugniasienių tipais. Apžvelgiama dažniausiai pasitaikančias ugniasienių apėjimo metodologijos. Ugniasienių metodologijos apėjimo aptikimo ir stabdymo skyriuje analizuojame kokios yra dažniausiai pasitaikančios ugniasienių apėjimo metodologijos ir kaip jas reikėtų sustabdyti. Pabaigoje yra pateikiamas literatūros sąrašas, kuriuo buvo remtasi rašant šį darbą.

Analizė

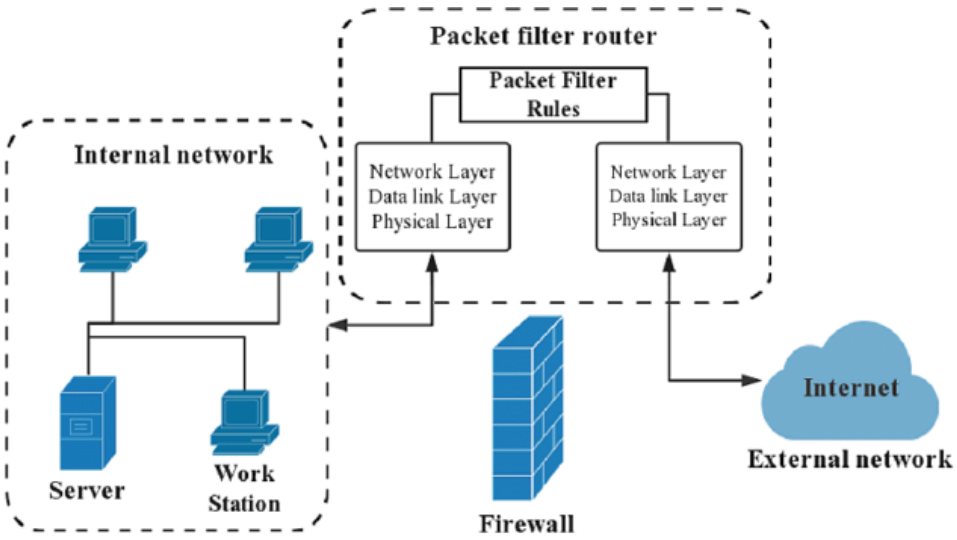
1.1. Ugniasienių tipai

1.1.1. Paketų filtravimo ugniasienės

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 [1]:

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

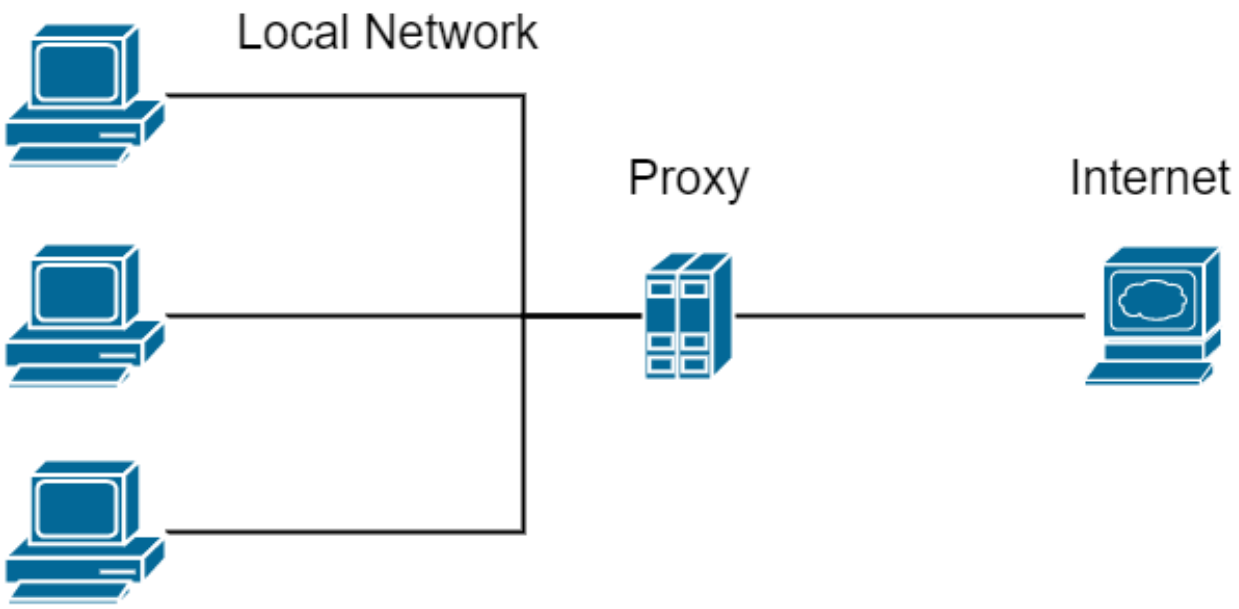
Paketus filtruojanti ugniasiene pirmiausia analizuoja paketų siuntėjo, ir gavėjo adresus, portus ir protokolus (pav. 1). Ugniasienes tikrina pagal analizuojamus kriterijus ir nusprendžia ar priimti paketą ar jį numesti pagal ugniasienes naudojamas taisykles.



pav. 1 Paprastos ugniasienes veikimo schema

1.1.2. Programos lygio šliuzų ugniasienės (angl. Application-level gateways 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).



pav. 2 Proxy ugniasiene

1.1.3. Naujos kartos ugniasienė (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 [2]. 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.

1.1.4. Busenos ugniasiene (angl. stateful inspection)

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 išsiųstam 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.

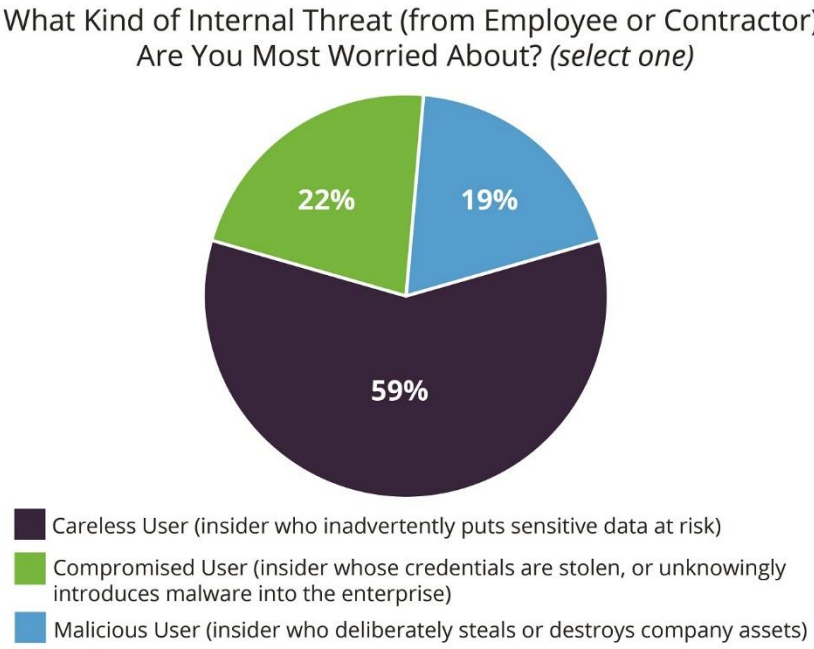
1.1.5. Grandinės lygio šliuzas (angl. circuit-level gateway)

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.

1.2. Pasitaikančios apėjimo metodologijos

1.2.1. Vidinės atakos

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



pav. 3 Kompanijų savininkų ir rangovų apklausa [3]

Buvo padaryta apklausa apie vidines atakas (pav. 3). Žmonės buvo klausinėjami kokių atakų labiausiai bijo. Daugiausiai bijo nesaugaus darbuotojo, kuris gali nežinodamas paskleisti kompanijos jautrius duomenis. Kompromituoti naudotojai, kurie pametė savo duomenis, arba jų duomenys buvo nulaužti surinko panašų procentų kiekį kaip ir naudotojai, kurie specialiai laužiasi į organizacijos tinklą, naudotojai kurie vagia duomenis arba specialiai naikina sistemas.

1.2.2. Praleisti saugos pataisymai

Šita problema egzistuoja ne vien ugniasienėje, bet ir programose, 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 naudotojams. Saugos pataisa padeda apsaugoti naudotojo programinę įrangą nuo skylių kuriomis gali pasinaudoti įsilaužėliai. Neatnaujinama programinė įranga gali būti nesaugi, kadangi atsiranda naujų pažeidimų kuriais įsilaužėliai 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.

1.2.3. Konfigūracijos klaidos

Ugniasienės blogos konfigūracijos klaidos pasitaiko dažnai. Net jei ir ugniasienė yra sukonfigūruota ji gali būti neveiksminga, arba tik dalinai veiksminga. Dažniausiai yra penkios problemos ugniasienės konfigūravime [4].

1. Blogai sukonfigūruota 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.

2. 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.

3. 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.

4. Nesukonfigūruotas išėjimo filtras

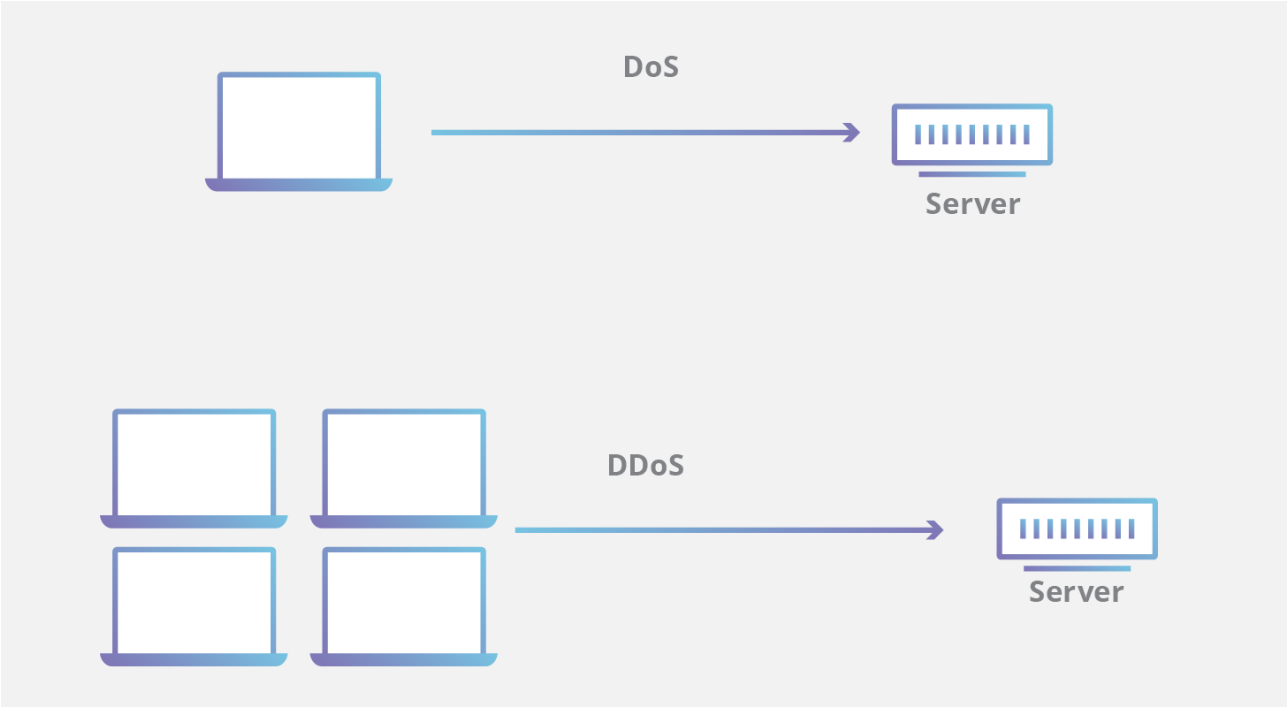
   Dažniausiai ugniasienės nėra filtruojamas išėjimo filtravimas. Naudotojas gali išsiūti bet kokią užklausą kur tik nori. Tai leidžia naudotojui lankytis nesaugiuose puslapiuose, ar tai leidžia parsisiųsti virusus, apie kuriuos gali pats naudotojas nežinoti.

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

   Sukonfigūravus ugniasienę tvarkingai, peržiūrėjus visas taisykles, neleidžiant visiems prisijunkit 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.

1.2.4. 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).



pav. 4 DoS ir DDoS

1.2.5. Socialinė inžinerija

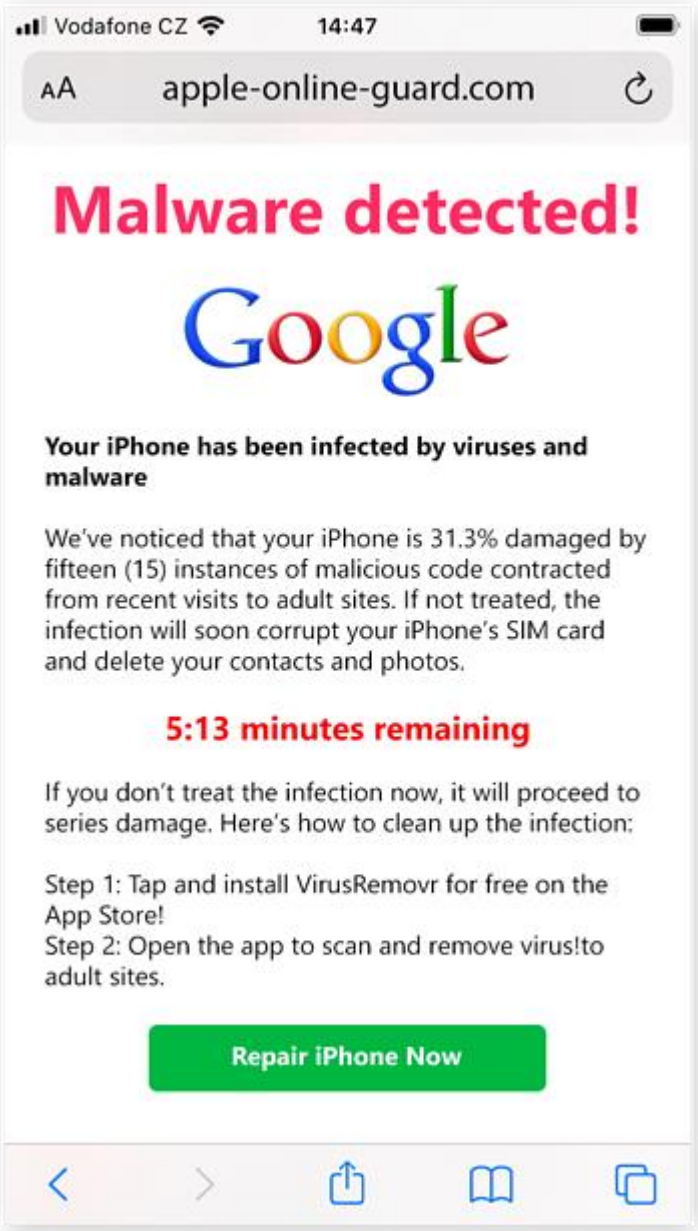
Socialinė inžinerijos ataka yra labiausiai paplitusi internete. Šitame spektre yra ne viena ir ne dvi atakos. Socialinė inžinerija yra tokios atakos kurios yra kompiuterio naudotojui. Tokios atakos gali remtis naudotojo jausmais, bandant apgauti naudotoją, ar bandant išgauti kažkokią informaciją, kuri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

1.2.6. Kibimas (angl. 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 naudongo naudotojui, kad jis 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.

1.2.7. Baidyklė (angl. 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 (pav. 5).



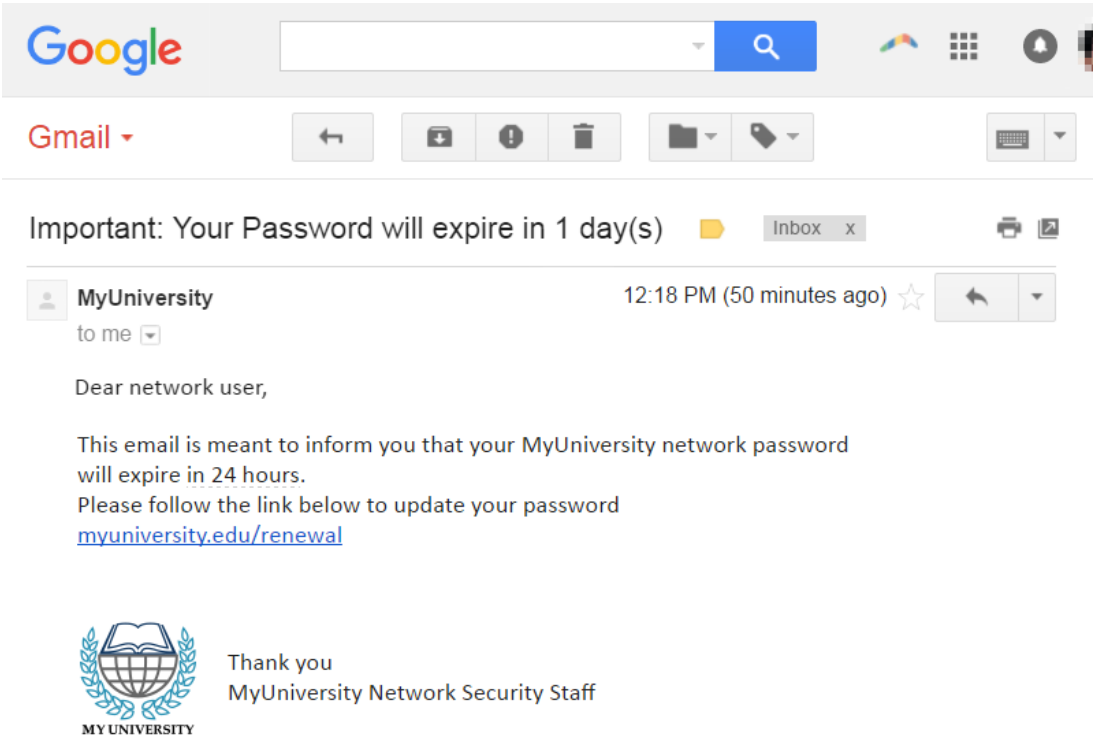
pav. 5 Baidyklė atakos pavyzdys

1.2.8. Pretekstas (angl. pretexting)

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

1.2.9. Sukčiavimas (angl. phishing)

Dažniausia ataka internete. Tokios atakos pasitaiko kiekvieną dieną. Dažniausiai yra atsiunčiamas elektroninis laiškas prašant atnaujinti slaptažodį ar atnaujinti kitą informaciją (pav. 6). 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.



pav. 6 Phishing atakos pavyzdys

1.2.10. Ieties sukčiavimas (angl. 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.

1.3. Vidinės atakos (angl. 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.

1.4. Praleisti saugos pataisymai

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.

1.5. Konfigūracijos klaidos

Ugniasienės konfigūracijos klaidas yra sunku aptikti, kadangi jas padaro žmogus kuris konfigūruoja. Tokias klaidas galima aptikti tik žmogui kuris tikrina ugniasienės klaidas. Norint aptikti tokias klaidas, specialistas turi patikrinti visą ugniasienės konfigūraciją. Tokių klaidų galima išvengti konfigūruojant ugniasienę naudojant, konfigūracijos gaires. Sukonfigūruotą ugniasienę su klaidom, dažniausiai būna sunku sutvarkyti, kadangi viso tinklo prieiga yra priklausoma nuo ugniasienės.

1.6. DoS ir DDoS atakos

Dažniausiai DoS arba DDoS atakoms aptikti yra naudojama speciali programinė įranga kuri analizuoja tinklą. Tokias atakas gali aptikti ir saugos specialistas, pamatęs, kad tinklas neveikia taip kaip turėtų veikti. DoS ataką galima lengvai sustabdyti, kadangi ji yra inicializuojama iš vieno ip adreso. Užblokavus aptiktą IP adresą tokia ataka būna sustabdoma. DDoS ataka yra ne iš vieno IP adreso, todėl tokios atakos stabdymui neužtenka užblokuoti vieno IP adreso. DDoS atakų sustabdyti neina, bet galima sumažinti jų žalą gerai sukonfigūravus ugniasienę ir padidinus tinklo pralaidumą jei yra galimybė.

1.7. Socialinė inžinerija

Tokias atakas nėra labai sunku atpažinti, bet naudotojas turi būti su jomis susipažinęs. Gavus elektrinį laiškai ar kitokiais būdai gavus žinutę reikėtu ją išanalizuoti. Dažniausiai tokios atakos yra siunčiamos, netikrais elektroninio pašto adresais arba įsilaužėlių perimtais el laiškais. Pirmiausia reikėtų išanalizuoti ar gauta žinutė yra iš patikimo šaltinio. Įsilaužėlis gali bandyti apsimesti žinomomis kompanijomis arba tikrais asmenimis. Reikėtų įsitikinti, kad žinutė yra gauta tikrai iš asmenis kuris yra realus ir jeigu eina patikrinti ar nebuvo nulaužtas naudotojo susisiekimo būdas. Tokiose žinutėse dažniausia yra prašoma pinigų ar kitokios informacijos. Būna atsiunčiamos žinutės kuriuose yra nuorodos arba failai. Reikėtų įsitikinti ar tokios nuorodos yra tikros. Gautus failus reikėtų išanalizuoti prieš juos atidarant. Apsisaugoti nuo tokių atakų yra sunku, jei naudotojas nėra susidūręs su tokiomis atakomis, todėl gavus žinutę reikėtų neskubėti ir išanalizuoti ją. Tokios atakos nebūtinai yra atliekamos žinučių principu, tokias atakas galima atlikti tiesiog bendraujant su asmeniu. Tokiais atvejais reikia stengtis neskleisti savo informacijos kaip prisijungimų ar kitos informacijos kuri gali būti panaudojant atakai.

Apibendrinimas ir išvados

Apibendrinus, galime teigti, kad yra daug skirtingų ugniasienės tipų ir jos atakų būdų. Atsirandant naujiems būdams apeiti ugniasienės, tokios atakos yra neišvengiamos. Ugniasienė gali tik sumažinti atakų kiekį. Norint labiau apsisaugoti nuo atakų reikia būti susipažinus su atakomis ir naudoti papildomą programinę įrangą kuri padėtų daugiau apsisaugoti nuo galimų ugniasienės apėjimų.

- Išanalizavus esamus ugniasienių tipus buvo pastebėta, kad jų yra labai daug. Nėra blogo pasirinkimo tarp ugniasienių. Tipo pasirinkimas turėtų būti nuspręstas pagal ugniasienės naudojimą. Vienos ugniasienės atakas valdo saugiau, kitos prasčiau.
- Išanalizavus pasitaikančias ugniasienių apėjimo metodologijas buvo pastebėta, kad jų yra įvairių. Vienai problemai gali būti daug sprendimo būdų, tokį patį pasakymą galima pritaikyti ir ugniasienės apėjimais. Yra daug būdų, kaip galima apeiti ugniasienę.
- Galima rasti daug būdų, kaip aptikti ir apsisaugoti nuo ugniasienės apėjimų. Kadangi yra daug skirtingų apėjimo būdų taip pat yra ir daug apsisaugojimo būdų nuo atakų.

Literatūros sąrašas

1. [1] 2. I. Upadhyay, „Packet Filtering Firewall All You Need To Know In 3 Easy Steps,“ 15 spalis 2020. [Tinkle]. Available: https://www.jigsawacademy.com/blogs/cyber-security/packet-filtering-firewall/. [Kreiptasi 14 lapkritis 2021].
3. [2] 4. C. EDU, „What is an Intrusion Prevention System (IPS)?,“ [Tinkle]. Available: https://www.forcepoint.com/cyber-edu/intrusion-prevention-system-ips. [Kreiptasi 15 lapritis 2021].
5. [3] 6. T. Casey, „Top Insider Threat Concern? Careless Users. [Survey],“ 12 liepa 2017. [Tinkle]. Available: https://www.imperva.com/blog/top-insider-threat-concern-careless-users-survey/. [Kreiptasi 12 Llapkritis 2021].
7. [4] 8. J. Edwards, „Five Firewall Configuration Mistakes You Need to Avoid,“ 24 sausis 2019. [Tinkle]. Available: https://www.networkcomputing.com/network-security/five-firewall-configuration-mistakes-you-need-avoid. [Kreiptasi 14 lapkritis 2021].