VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
KOMPIUTERIJOS KATEDRA

Darbo/ataskaitos tipas

Kibernetinio saugumo pažeidžiamos paslaugos ir atakos vektoriaus įgyvendinimo metodų tyrimas

Atliko:
Deividas Slauzgalvis parašas
Mindaugas Strakšys parašas

Vilnius
2018

dr. Vadovas Vadovaitis

Turinys

Sutartinis terminų žodynas

Pateikiamas terminų sąrašas (jei reikia)

Santrauka

Santraukos tekstas rašto darbo kalba...

Summary

Darbo pavadinimas kita kalba

This is a summary in English...

Įvadas

Įvado tekstas ...

1. Kibernetinio saugumo analizė

1.1. Kibernetinio saugumo apžvalga

1.1.1. Kibernetinio saugumo istorija

Kibernetinio saugumo industrija, kuri 2015 metais buvo verta 75 milijardų dolerių, prasidėjo 1988 metais, kai Robert T.Morris paleido savo replikuojantį "kirminą" ARPANET tinkle(interneto pradininkas). Šis "kirminas" buvo dalis projekto, kuris skaičiavo interneto dydį užkrėsdamas UNIX operacines sistemas tam kad suskaičiuotų jose esančių prisijungimų prie interneto kiekį. Dėl programavimo klaidos, "kirminas" pradėjo jungtis į tas pačias mašinas daugelį kartų, taip visiškai "užkišdamas" tinklus ir priverdamas sistemas "užlūžti", taip tapdamas pirmuoju tokio tipo įrankiu susilaukusiu didžiulo žiniasklaidos dėmesio. Jo kūrėjas buvo išmestas iš universiteto, nuteistas lygtinai trejiems metams bei nubaustas 10 000 dolerių bauda.
Paskutiniame 20a. dešimtmetyje virusai pradėjo smarkiai plisti internetinėje erdvėje, turbūt tada populiaurisi jų - **ILOVEYOU** ir **The Melissa** virusai. Jie užkrėtė dešimtis milijonų kompiuterių visame pasaulyje, privertė žlugti daugelį elektroninio pašto sistemų. Šie virusai pasižymėjo vienu įdomiu dalyku - jie neturėjo apibrėžto tikslo ir taikinio, ir nesiekė jokios finansinės ar politinės naudos. Vienintelis jų tikslas buvo sukelti paniką ir chaosą virtualioje erdvėje. Tam, kad pasipriešinti šiems virusams buvo pradėtos kurtis pirmosios sistemos, skirtos apsiginti nuo virusų (antivirusinės). Taipogi, kompanijos pradėjo šviesti ir edukuoti savo darbuotojus kibernetinio saugumo temomis. Jie buvo išmokyti neatidarinėti neaiškių elektroninių laiškų, tam, kad išvengti "phishing" tipo atakų. Būtent šiuo metu kompanijos rimtai susirūpino kibernetinio saugumo klausimais ir apie tai pradėta diskutuoti viešumoje.
21a. pirmajame dešimtmetyje kibernetinės atakos pasidarė dar rimtesnės ir pavojingesnės. Atakuoti buvo pradėtos kreditinės kortelės ir elektroninės banko sąskaitos. Tarp 2005 ir 2007 metų Albert Gonzalez su savo kibernetinių nusikaltėlių gauja sugebėjo pavogti informaciją iš bent 45,7 milijono kreditinių kortelių. TJX kompanija dėl to patyrė 256 milijonų dolerių nuostolį. Tai buvo puiki pamoka tiek TJX, tiek kitoms kompanijoms. Į kibernetinį saugumą reikėjo pradėti žiūrėti daug rimčiau nei ankščiau, nes tai praleidus pro akis nuostoliai gali būti milžiniški ir pasibaigti kompanijos bankrotu.
2014 metais kibernetiniai nusikaltėliai perėmė milžiniškus kiekius Sony bei Target kompanijų duomenų. Šįkart buvo taikytasį ne tik į finansinę naudą, bet ir į kompanijos reputaciją ir jos darbuotojų gerovę. Tačiau Target kompaniją dėl to prarado apie 162 milijonus dolerių ir daugelį klientų - nes nusikaltėliai turėjo prieigą prie 70 milijonų Target kompanijos klientų asmeninių duomenų. Taipogi nustatyta,kad už Sony kompanijos duomenų kompromitavimą atsakingą Šiaurės Korėja. Taigi, kibernetinės atakos tapo ne tik finansinės naudos siekimo įrankiu, tačiau ir stipriu politiniu(teroristiniu) įrankiu, skirtu aiškintis nesutarimus tarp šalių. Kuo technologijos modernesnės, tuo daugiau naudingos ir svarbios informacijos ten talpinama. Dabar kibernetinė sauga yra vienas svarbiausių prioritėtų kompanijose. Ir tuo rūpintis reikia, kol atakos dar neįvyko (išankstinė atakų prevencija), nes atakos eksplotavimo metu gintis jau per vėlu ir nuostaliai gali būti tragiški.

1.1.2. Kompiuterinių sistemų atakavimo apžvalga

Kiekviena kompiuterinė sistema turi trukumų, kuriuos anksčiau ar vėliau atranda programuotojai. Tokių trūkumų ieškotojai dalinami į du tipus - vieni stengiasi tam tikrą sistemą sutvirtinti atradus spragų, kiti tai daro tūrėdami kenkėjiškų motyvų [Motivations behind attacks]. Tačiau trūkumo

ieškojimas nėra paprastas procesas, jis susideda iš daugybės etapų, kurie kas kart gali skirtis dėl skirtingų atakų tipų. Tačiau kiekvienos atakos pradinis taškas, nuo kurio prasideda atakos planavimas, yra pasiruošimo stadija.

Kibernetinių atakų pasiruošimo stadijoje svarbiausias žingsnis yra susipažinimas su sistema, kurią ruošiamsi atakuoti. Šiame etape svarbu susipažinti su sistemos aukos architektūra, naudojamas programas, kokių technologijų pagalba ši sistema egzistuoja internetinėje erdvėje, sistemos IP adresus ar betkokią kitą su sistema susijusią informaciją, kuri galėtų padėti lengviau ir saugiau užkrėsti sistemą. Sistemos architektūros analyzavimas gali prasidėti nuo informacijos ieškojimo aukos sistemos socialiniuose puslapiuose ar net meginant susisiekti su asmenimis atsakingais už sistemos priežiūrą ir taip išgauti reikiamų duomenų.

Sisipažinus su atakuojama sistema kitas žingsnis yra sistemos skanavimas naudojant konkrečius tinklo ir jame esančių paketų analizavimo įrankius. Tokiems įrankiams dažnu atveju reikalingas aukos sistemos IP adresas, su kuriuo pagalba analizavimo įrankis sužinotu plačiau apie techninę sistemos veikimo pusę. Išgautoje informacijoje galima aptikti naudojamą operacinę sistemą, naudojamų programinių įrankių versijas, maršrutizatoriaus lenteles(angliškai. routing tables). Visa analizavimo įrankio surinkta informacija leidžia susidėlioti konkretesnį atakuojamos sistemos architektūros braižą ir suteikia galimybę lengviau atrasti sistemos saugumo spragų.

Pasinaudojus išgauta informacija vienas iš dažniausių būdų užpulti sistemą yra pasinaudojimas atakuojamos sistemos naudojamų programinių įrankių saugumo spragomis. Pagal naudojamą programinės įrangos versija internete galima surasti jau atrastas saugumo spragas ir jomis pasinaudoti. Vienos saugumo spragos padeda padaryti nedaug žalos, tačiau su kitomis galima išgauti privačios informacijos.

1.1.3. Kompiuterinių sistemų saugumo apžvalga

Internetas, tai vieta, kur dažnu atveju vartotojas pervertina savo saugumą, be išankstinio pamąstymo naršo interneto platybėse bei talpiną asmeninę informacija. Tačiau tai nėra saugi aplinka, o ypač pavojinga, nes nuo kimbernetinių atakų nė vienas kompiuterio vartotojas negali apsisaugoti visu šimtu procentu. Tačiau yra būdų, kurie padėtų atakos riziką sumažinti ar net privestų atakuotuojus nuleisti rankas.

Vienas iš svarbiausių būdų apsisaugoti nuo programuotojų, kurie rengia kibernetines atakas, yra naudojamos programinės įrangos naujinimas, kai tik nauja versijas yra išleista. Kad nepraleisti programinės įrangos naujinimų svarbu palaikyti automatinio atnaujinimo funkciją naudojamose programėlėse. Nuolatinis programinės įrangos atnaujinimas yra svarbus tuom, kad naujesnė produkto versija nebeturi senesnių versijų saugumo trukumų, kurie buvo atrasti saugumo specialistų. Taip pat užtrunka, kol programuotojai atranda saugumo spragas tik išleistoje versijoje. Taigi tai yra vienas iš svarbesnių būdų atbaidyti kenkėjus.

Kitas svarbus ir dažnas atakavimo būdas naudojant susisiekimo priemones. Šiuo atvėju svarbu apsisaugoti nuo programuotojų, kurie nori išvilioti jūsų prisijungimo duomenis komunikacijos pagalba. Tai dažniausiai yra daroma naudojant elektroninį paštą. Šiuo būdų vartotojas gauna labai oficialią žinutę, kuri iš tikrūjų yra suklastota. Žinutėje dažniausiai stengiamasi nuvilioti į programuotojų svetaines, kur programuotojas mato visus aukos vykdomus procesus. Taip pat žinutė gali talpinti užkrėstas programas ar tiesiog prašyti asmeninės informacijos. Kita susisiekimo priemonė, kurią naudoja atakų kūrėjai yra mobilus telefonas. Pasinaudojus šiuo įrenginiu atakų kūrėjai apsimeta tam tikros kompanijos atstovu ir taip megina išvilioti aukos informaciją. Šiuo atvėju svarbu išlaikyti blaivų protą, kai komunikacijos pagalba norima sužinoti svarbią asmeninę

informaciją.

Taip pat populiarus būdas programuotojams sužinoti slaptos informacijos yra bevielis ryšys. Juo pagalba programuotojai viešose vietose ieško neapsaugotų elektroninių prietaisų naudojančių Wi-Fi technologiją. Antivirusinės programos dažnai apsaugo nuo šių atakų, tačiau svarbu būti atsargiems naudojantis atviru Wi-Fi signalu, o privačių naršymo procesų atlikimas, pavyzdžiui elektroninės bankininkystės naudojimasis ar kompanijos duomenų persiuntimas, tūrėtų būti paliktas tik ypač saugiems interneto tinklams(namų, įmonės internetinis ryšys).

Svarbu tai, kad atliekami procesai naudojantis internetinį ryšį ar komunikacijos platformas būtų apgalvoti ir atsakingi. Net paprasčiausias mobilaus telefono numerio nutekinimas ar viešas paskelbimas gali pridaryti žalos numerio savininkui. Todėl svarbu užtikrinti ir įsitikinti, kad slapta kompiuteryje ar internetinėje erdėje laikoma informacija yra saugi ir prieinama tik asmenims tam turintiems teisę.

1.2. Pagrindiniai kibernetinių atakų tipai

Kibernetinėje erdvėje kiekvieną dieną vyksta daugybę kibernetinių atakų. Kadangi kiekviena internetinė sistema yra skirtinga ir naudoja vis kitokias programines įrangas, todėl ir kiekvienos atakos tipas yra kitoks priklausomai nuo sistemos trūkumų ar net atakos kūrėjo motyvų. Pagal kovo mėnesį užfiksuotas atakas "HACKMAGEDDON" sudarė statistiką [Attack Vectors], kurioje atakų vektorius suskirstė į šešis skirtingus tipus, kurie apibūdina visas to mėnesio vykusias kibernetines atakas. Kadangi puolimo tipų yra begalo daug, šiame poskyrije nagrinėjami dažniau naudojami konkretūs puolimo tipai.

1.2.1. SQL injekcijos

1.2.2. XSS injekcijos

1.2.3. Phishingas

1.2.4. Kenkėjiškos programos

Kenkėjiškas programas galima skirstyti į tris pagrindines kategorijas:
1) Virusus
2) Kirminus
3) Trojos arklius
Nors visi jie skirti užkrėsti bei kompromituoti sistemą, kiekviena kategorija turi esminių skirtumų.

Virusas – tai kenkėjiškas kodas, prikabinamas prie įvairių failių – dažniausiai .exe (executable) tipo failų. Pagrindinis virusų trūkumas yra tai, kad jie negali aktyvuotis bei plisti be jokio vartotojo įsikišimo. Tam, kad virusas pradėtu plisti būtina sąsaja tarp vartojo ir komputerio. Tam, kad virusai plistu iš kompiuterio į kompiuterį, kompiutero vartotojas pats turi jį nusiųsti (sąmoningai arba ne) elektroniniu paštu ar kitais failų per tinklą dalinimosi metodais. Virusu darom žala gali būti įvairi, pradedant tiesiog kompiuterio sulėtinimu, baigiant programinės įrangos (o kartais ir vadinamasios „geležies“ (angl. „hardware“) bei failų sugadinimu nepataisomai.

Kirminai iš esmės gan panašus į virusus, kartais net laikomi virusu „sub“ kategorija. Kirminai iš kompiuterio į kompiuterį gali plisti daug lengviau nei virusai – jiem nereikia žmogaus įsikišimo. Kirminai patys sugeba skleisti ir platinti save tinkle. Vienas kirminas esantis kompiuteryje gali save paplatinti tinkle šimtus tūkstančių ar net milijonus kartu – todėl kirminai daug pavojingesni negu paprasti savęs platinti tinkle negalintys virusai. Save duplikuodami kirminai sunaudja labai

didelius kompiuterio bei tinklo resursus, taip priversdami kompiuterius, web serverius bei tinklų serverius lėčiau veikti ar nustoti veikti visiškai.

Trojos arkliu vadinama kenkėjiška įranga, kuri apsimeta esanti tuo, kuo ištikrūjų nėra. Taip pavadinta dėl Trojos arklio mito. Dažniausias trojos arklys kompiuteryje apsimeta esąs naudinga programina įranga, tačiau įjungtas daro įvairią žalą kompiuteriui. Trojos arkliai dažniau būną tiesiog įkyrus negu kenksmingi, bet būna ir išimčių – kartais jie gali ištrinti arba užkriptuoti informaciją esančia kompiuteryje. Nemaža dalis Trojos arklių taip pat gali veikti pasiremdami „backdoor“ principu, atverdami prieigą prie kompiuterio įsilaužėjams ar kitiems kenkėjiškų tikslų turintiems asmenims. Skirtingai nei virusai ar kirminai, Trojos arkliai savęs neduplikuoja kituose kompiuteriuose ar sistemose.

1.2.5. Slaptažodžių laužimas

1.2.6. DDOS/DOS atakos

2. Pasirinktų atakos vektorių analizė

3. Pasirinktų atakos vektorių implementacija

- neveike virtaulke neleido parsiusti (control panel) -install (duombaze, duombazei reik microsoft visual)

4. Šaltiniai

Išvados ir rekomendacijos

Išvados bei rekomendacijos.

Ateities tyrimų planas

Pristatomi ateities darbai ir/ar jų planas, gairės tolimesniems darbams....

Priedai

Dokumentą sudaro du priedai: A priede ....

A. Pirmojo priedo pavadinimas

Pirmojo priedo tekstas ...

B. Antrojo priedo pavadinimas

Antrojo priedo tekstas ...