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. 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.

1.2. Pagrindiniai kibernetinių atakų tipai

1.2.1. SQL injekcijos

1.2.2. XSS injekcijos

1.2.3. Phishingas

1.2.4. Kenkėjiškos programos

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 ...