VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
INFORMATIKOS INSTITUTAS
KOMPIUTERINIO IR DUOMENŲ MODELIAVIMO KATEDRA

Bakalauro darbas

Saugus pažeidžiamumų skaitytuvas sistemų auditavimui

Atliko:
Jonas Gavėnavičius parašas

Vadovas:
Lektorius Virgilijus Krinickij

Vilnius
2019

Turinys

Sutartinis terminų žodynas

Pateikiamas terminų sąrašas (jei reikia)

Santrauka

Šiais laikais kai pasaulis tampa vis labiau ir labiau skaitmenizuotas, iškyla pati opiausia problema, tai yra kibernetine sauga. Vis daugiau pavyždžių matome kaip įsibrauna į sistemas kurias galima potencialiai išnaudoti dėl finansinių ar kitų priežasčiu. Taip pat dėl to nukenčia ir tų sistemų vartotojai - finansiškai ar morališkai, jų privati informacija būna pavogiama ir paviešinama. Niekas nėra saugus nuo tokių situacijų. Todėl valstybės, įmonės ar korporacijos vis daugiau investuoja į kibernetinę apsaugą, kibernetinė sauga tampa vis dažnesnė diskusija visuomenėja, vis daugiau dėmėsio ir resursų skiriama butent jai, stengemasi užkirsti kelią minėtoms situacijoms. Kuriami įrankiai kurie analizuoja sistemas ir randa jų spragas, pritaikomos įvairios technologijos ar metodai kurie perspėja apie galima ar vykstančią ataką prieš sistemą, stengiamasi rasti sistemoje spragas ir užlopyti jas kol jų nerado asmenys kurie išnaudotų jas.

Summary

Darbo pavadinimas kita kalba

This is a summary in English...

Įvadas

Šiame darbe kuriamas saugus įrankis, kuris neišduotų savo serverio vietos ir vartotojai pasinaudoje juo galėtų gauti išsamią informacija apie jų internetinėje svetainėje egzistuojančias spragas, bei pažeidžiamumus ar modifikuotus failus. Darbo tikslas - Sukurti saugų pažeidžiamumų skanavimo įrankį, kuris pasileistų iš tam tikros VPN technologija slepiamos vietos, skanuotų internetinę svetainė, bei jos failus, aptiktų pažeidžiamumus ar modifikuotus failus, ir pateiktų klientui informaciją apie skanavimo rezultatus. Siekiant kad darbas būtų paklausus ir veiksmingas, keliami šie darbo uždaviniai:

1. Apžvelgti egzistuojančius panašius įrankius;
2. Išanalizuoti dažniausiai pasitaikančius internetinių svetainių pažeidžiamumus;
3. Išanalizuoti dažniausiai pasitaikančių pažeidžiamumų egzistuojančius atviro kodo įrankius;
4. Išanalizuoti dažniausiai pasitaikančius internetinių svetainių skanavimo metodus.

Kibernetinis saugumas yra svarbi kiekvienos sistemos dalis. Kadangi kiekvieną sistemą kuria žmogus, į kiekvieną sistema įeina žmogiškasis faktorius, del kurio sistemos beveik visada turi pažeidžiamumų kuriuos gali išnaudoti puolėjas siekiantis tam tikros naudos. Dėl šios priežasties toks įrankis būtų ypač naudingas bet kokiai sistemai. Aptikus pažeidžiamumą, galima įtarti, kad ta pažeidžiamuma gali aptikti ir nuostolio siekiantys asmenys, arba jį jau buvo aptiktas, ir tam tikri failai buvo modifikuoti įdedant tam tikrą kodą kuris leistų atakuojančiui asmeniui patekti į sistemą nepastebėtam. Dėl šių priežasčių, saugus ir automatizuotas sistemų pažeidžiamumo skanavimo įrankis yra ypač aktuolus. Tačiau šio įrankio kurimą yra apsunkina šios priežastys:

- Įrankio kurimas reikalauja didelio bagažo žinių;
- Dauguma sistemų kurios turi pažeidžiamas vietas nera atviro kodo, todėl ne visada įmanoma aptikti kas būtent sukelią šį pažeidžiamumą, ar išvis kad egzistuoja toks pažeidžiamumas bei pažeidžiamumas būna aptinkamas daug vėliau negu atviro kodo pažeidžiamumai;
- Sistemoje gali būti tiek daug skirtingų potencialių pažeidžiamų, kad jų aptikimo automatizavimas tampa galimai neįmanomas.

Šias problemas siuloma spresti apskaičiuojant tam tikrą įrankio veiksmingumą procentaliai. Didžiausias tokio sprendimo privalumas yra tas kad vartotojas supras, kad tokio įrankio rezultatų analizavimas ir pritaikymas neužtikrina visų pažeidžiamumų aptikimo ir kibernetinio saugumo užtikrinimo. Šio įrankio kurimo metu, siekiant sukurti saugų pažeidžiamumų aptiko įrankį, siekiama pagerinti sistemos saugumą, bet neužtikrinti jo. Įrankis bus skirtas tik internetinėms svetainėms ir nebus stengiamasi jį pritaikyti ir kitoms sistemoms.

1. Susijusių darbų analizė

1.1. Internetinių svetainių spragų skaitytuvai

1.1.1. Pentest-Tools skaitytuvas

Pateikiamas trečio lygio poskyrio tekstas.

2. Sistemų auditavimas

2.1. Elgsenos analizė

2.1.1. Example

Pateikiamas trečio lygio poskyrio tekstas.

2.2. Statinė spragų analizė

2.2.1. Example

Pateikiamas trečio lygio poskyrio tekstas.

2.3. Dinaminė spragų analizė

2.3.1. Example

Pateikiamas trečio lygio poskyrio tekstas.

2.4. Išorinių spragų skanavimas

2.4.1. Example

Pateikiamas trečio lygio poskyrio tekstas.

2.5. Vidinių spragų skanavimas

2.5.1. Example

Pateikiamas trečio lygio poskyrio tekstas.

2.6. Aplinkos spragų skanavimas

2.6.1. Example

Pateikiamas trečio lygio poskyrio tekstas.

3. Gerosios praktikos

3.1. Atviros kodo programinė įranga

3.1.1. Privalumai

Pateikiamas trečio lygio poskyrio tekstas.

3.1.2. Trūkumai

Pateikiamas trečio lygio poskyrio tekstas.

3.1.3. Apibendrinimas

Pateikiamas trečio lygio poskyrio tekstas.

3.2. Uždaro kodo programinė įranga

3.2.1. Privalumai

Pateikiamas trečio lygio poskyrio tekstas.

3.2.2. Trūkumai

Pateikiamas trečio lygio poskyrio tekstas.

3.2.3. Apibendrinimas

Pateikiamas trečio lygio poskyrio tekstas.

4. Sistemų auditavimo įrankis

4.1. Įrankio aprašas

Pateikiamas 4.5 poskyrio tekstas. Vienas iš šaltinių [?]. Visas turinys priklauso 4 skyriui.

4.2. Aptiktini pažeidžiamumai

Pateikiamas 4.5 poskyrio tekstas. Vienas iš šaltinių [?]. Visas turinys priklauso 4 skyriui.

4.3. Tikslumas

Pateikiamas 4.5 poskyrio tekstas. Vienas iš šaltinių [?]. Visas turinys priklauso 4 skyriui.

4.4. Įgyvendinti lukeščiai

Pateikiamas 4.5 poskyrio tekstas. Vienas iš šaltinių [?]. Visas turinys priklauso 4 skyriui.

4.5. Trūkumai

Pateikiamas 4.5 poskyrio tekstas. Vienas iš šaltinių [?]. Visas turinys priklauso 4 skyriui.

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 ...