Reputácia sieťových entít v kontexte manažmentu bezpečnostných informácií a udalostí

Judita Jusková

3Ib, 2016 - 2017

Abstrakt. Škodlivý kód, malware alebo spam, ktorý je vykonávaný na počítačoch môže poskytnúť širokú škálu útokov na dostupnosť siete alebo napadnutia súkromia a dôvernosti užívateľov. V tejto práci sme sa zamerali na sumarizáciu známych sieťových entít a meraní reputačného skóre, ktoré vyjadruje stupeň ohrozenia z jednotlivých IP, DNS a emailových adries. Taktiež porovnávanie prístupov k tvorbe reputácií sieťových entít a navrhnutie programu.

Kľúčové slová: reputácia IP, reputácia DNS, reputácia sieťových entít

1 Úvod

Sieťová bezpečnosť je jedna z oblastí informatiky. Definuje sa ako zabezpečenie sieti a sieťových zariadení. Poskytuje nepretržité služby pre oprávnených používateľov, prevenciu odcudzenia dát alebo aj kontrolu neoprávneného prístupu. Sieťová bezpečnosť súvisí aj so zabezpečením proti rôznym sieťovým útokom.
Aj keď to nevnímame, reputačné systémy ovplyvňujú náš život každý deň. V bežnom živote nás obklopuje povesť, ktorá je veľmi dôležitá preto, že ju môžeme využívať pri dôležitých rozhodnutiach v reálnom živote. Takáto povesť/ reputácia je ešte dôležitejšia a užitočnejšia na internete. Každý deň pribúda na internete mnoho nových stránok, a každá z nich bojuje o pozornosť bežných užívateľov. Ako majú užívatelia vedieť, že stránka je bezpečná a nesnaží sa len o útok? V minulosti reputačné systémy neexistovali a neboli ani potrebné, pretože webových stánok, útočníkov, hackerov bolo na svete málo. V dnešnej dobe sú takéto systémy už neodmysliteľnou súčasťou, stávajú sa základným prvkom dôvery a bezpečnostnej architektúry akéhokoľvek systému, používateľa alebo služby.

V dnešnej dobe si sieťoví operátori čoraz častejšie vyžadujú monitorovanie ich siete. Je to hlavne kvôli správnemu zabezpečeniu takejto siete. Na monitorovanie sú rozmiestnené rôzne detektory škodlivých a nevyžiadaných prístupov. Takéto systémy môžu pomôcť včas varovať pred nebezpečnými udalosťami.

Detektory nemusia byť len v jednej lokálnej sieti, informácie môžu medzi sebou zdieľať viacero organizácii. Záznamy sa takto môžu niekoľko násobne zväčšiť a tým napomáhať upresňovaniu škodlivých činností. Zo záznamov sa môžu získavať zaujímavé vlastnosti škodlivých prevádzok. Následné získané odhadovanie miery hrozby, tzv. *povestné skóre* [3].

Sieťová bezpečnosť sa týka zabezpečenia sieti a sieťových zariadení. Rieši aj poskytovanie nepretržitej služby pre oprávnených užívateľov. S tým súvisí aj zabezpečenie proti rôznym sieťovým útokom. V dnešnej dobe sa na internete pohybuje veľa užívateľov a s nimi aj IP adries. Niektoré IP adresy sú bezpečné, iné naopak menej bezpečné. Takýmto škodlivým IP adresám je najlepšie sa vyvarovať. Na internete vzniká mnoho blacklistov, ktoré majú riešiť tento problém. Prospešné pre človeka, majú byť v tom, že sa v nich môže dopátrať k zlým, škodlivým IP adresám, ktoré boli už v minulosti označené, že sú nevhodné.

V práci sme najprv analyzovali postupne takéto blacklisty a reputačné systémy, ktoré sa snažia informovať užívateľov o škodlivých IP adresách a tak zabezpečovať siete. Zamerali sme sa na takúto reputáciu a snažili sme sa vytvoriť systém. K tomuto systému by mal prístup hocikto, kto by potreboval zistiť informácie o rôznych IP adresách. V práci hľadáme kompletné informácie o IP adresách. Nie len aké hodnotenie/ povesť Vaša IP adresa na internete má, ale aj geografické súradnice danej adresy, polohu, zoznam blacklistov, v ktorých sa adresa nachádza, celkov počet, koľko krát sa IP adresa v blacklistoch nachádza, atď..

1.1 Reputácia

Približne pred 15 rokmi, nebolo dostatočné množstvo informácií na digitálne ohodnotenie kvalít určitého subjektu. Kedysi sme si reputácie subjektov budovali sami. Tým, že sme informácie o subjekte zisťovali od spolupracovníkov, priateľov a rodiny. Naša schopnosť ťažiť informácie mala obmedzené zdroje. Jediné zdroje boli so svojich rodinných a spoločenských kruhov. Na základe zistených pozostatkov si potom každý subjektívne vytvoril názor, inými slovami subjektívnu reputáciu objektu.

1.1.1 Definícia reputácií

Základná vec pri navrhovaní prístupu je formálna definícia významu reputácie, reputačného systému a reputačného skóre. Ako uviedli v práci [3] slovo "reputácia" definuje spoločnú mienku, ktorú majú subjekty o objektoch. Je založená na spoločnom zdieľaní názorov o objekte, skúsenosti s nimi a doterajšom správaním sa objektu, resp. subjektu.

1.1.2 Reputačné skóre

Reputačné skóre je definované ako pravdepodobnosť, že subjekt bude vykonávať škodlivú činnosť v blízkej budúcnosti, na základe jeho správania v minulosti. Reputačné skóre je založené na predpokladoch budúcich útokov. Preto je vhodné definovať prístup k predikcii.

Vstupom do algoritmu predikcie bude súhrn všetkých škodlivých udalostí za určité uplynulé obdobie. Môže byť dopĺňané rôznymi ďalšími vstupmi ako štatistika o možno riziku. V našej práci to budú rôzne vstupy ako krajina, mesto, systém, ktorý

zisťuje či je uvedená IP adresa na niektorých zoznamoch blacklistov, či má statický alebo dynamicky priradenú IP adresu.

1.1.3 Význam reputácií

Reputačný systém predstavuje významný trend v rozhodovaní sa o dôvere subjektov na Internete. Základnou myšlienkou takýchto reputačných systémov je ohodnotenie subjektov napríklad na základe vykonaných transakcií alebo akejkoľvek aktivite na internete. Zistené informácie následne použiť na agregované hodnotenia daných subjektov. Týmto je možné odvodiť dôveru subjektu, ktoré môže pomôcť ostatným stranám pri rozhodovaní sa, o interakciu so subjektom v budúcnosti.
Reputácia je založená na tom, že má zhromažďovať, ukladať, aktualizovať A distribuovať povesť a informácie o adrese. Databáza určuje architektúru systému a ukladá všetky získané informácie do centrálneho úložiska
Zámerom reputácií je umožniť zdieľanie informácií veľkého množstva adries. Systém môže pôsobiť pozitívne alebo aj negatívne, keďže je nutné klasifikovať jednotlivé detaily a informácie o adresách. Technicky si vykonávanie takéhoto systému vyžaduje 3 základné body [5]: integrácia vhodných prostriedkov, vhodné rozbočovače a protokol, ktorý umožní komunikáciu medzi jednotlivými bodmi.

1.1.4 Reputácie sieťových entít

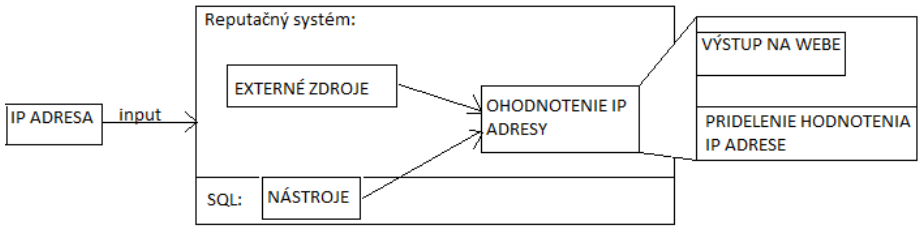
Termín reputácia sa chápe, z oblasti sociálnych sietí a virtuálnych komunít, ako dôkazy o správaní sa objektu v minulosti a následné podľa zistených informácií predpokladanie správania sa objektu v budúcnosti. Na výsledky vplývajú aj vzťahy k iným objektom. V práci sa zaoberáme reputáciou sieťových entít. Znamená to, že riešime viacero vstupných elementov. Elementom alebo entitou v našej práci je reputácia IP adries, bežných užívateľov na internete a reputácia DNS domén.
IP reputácia je jedným z tradičných metód pre rozpoznávanie zakázaných alebo škodlivých IP adries. Znamená to, či sú IP adresy známe tým, že sú zdrojom spamu alebo či súvisí s nejakou hrozbou malweru. Používanie IP reputácií rapídne rastie tým, že sa filtrujú rôzne informácie o IP adrese do výsledného hodnotenia.
Všetka pošta musí pochádzať z IP adresy a IP reputácia môže byť použitá na zistenie, či IP adresa je zodpovedná za rozosielanie spamu alebo nechcených hromadných e-mailov. Je to mimoriadne účinné, pretože takýto reputačný systém dokáže identifikovať až 80-90% útočníkov. Dôležitým faktorom pri systéme je to, kto je vlastníkom danej IP adresy a teda kto je zodpovedný za činnosť IP adresy na internete. Existuje mnoho firiem a zdrojov, ktoré sa snažia sledovať rôzne typy správania IP adries na internete. Tým sa snažia vyvíjať zoznamy IP povestí. Tieto systémy sú neskôr používané k úplnému filtrovaniu prichádzajúcich e-mailov z danej IP adresy. Systémy sú zostavené z dát, ktoré ukazujú, že IP adresa je zodpovedná len za určité typy správania sa na internete.
Niektoré zo záznamov reputácií sú voľné dostupné, za iné si treba mesačne zaplatiť. Existujú aj systémy, ktoré nie sú vôbec prístupné verejnosti ani po zaplatení. Nazývajú sa komerčnými reputáciami a sú určené len na súkromne účely povoleným osobám. Zaujímavé na reputačných systémoch je, že ak majú spoločnosti slabšie

zabezpečenie, takéto systémy sú na prvom mieste v detekcii nežiadúcich IP adries. Aby sa tak vyhli akémukoľvek preniknutiu do siete alebo spoločnosti.

Reputácia DNS je nevyhnutnou súčasťou internetovej infraštruktúry, ktorá realizuje preklad názov domén na IP adresy Incidenty, ktoré sa odohrávajú v poslednom období, využívajú DNS na páchanie obrovských škôd a škodlivých aktivít na internete. Preto detekcia škodlivých domén predstavuje dôležitú úlohu pri lepšom zabezpečení, samotného internetu, ale aj sieti na internete. Je pravdepodobné, že doména [6], ktorá je príbuzná so škodlivou doménou, bude vykonávať škodlivú aktivitu na internete.
Termín doménová reputácia, predstavuje určitú mieru presvedčenia, že doména je čestná a bezpečná alebo škodlivá. Môže podporiť, rozhodovanie o blokovaní prevádzky alebo varovania organizácií o podozrivej aktivite domény. Dnes sú v prevádzke zoznamy domén, ktoré sú považované za bezpečne a sú publikované v o webových informačných spoločnostiach. Rovnako sú zaznamenávané aj malwérové domény, ktoré sú v čiernych listinách(blacklistoch) a sú publikované v analytických službách webových hrozieb.
Malwerové domény majú tendenciu používať DNS pre svoju škodlivú činnosť [7]:

- **Botnet C&C**: používa DNS na proxy komunikáciu z infikovaných zariadení do radiča botnetu
- **Drop zóna**: používa DNS na vyhľadávanie domén pre ukladanie ukradnutých dát
- **Phishing stránky**: používajú DNS na mapovanie známych domén aby oklamali obete útoku

1.2 Ilustračný príklad



Obrázok 1. Návrh reputačného systému

Vo všeobecnosti platí, že reputačný systém pristupuje k dátam z rôznych dátových zdrojov, kde posudzuje charakter IP adresy. V závislosti od nájdenia zhody zo záznamov z minulosti, sa zvyšuje váha priradenia hodnotenia k danej IP adrese. Na

obrázku 1. môžeme vidieť koncepčný model, znázorňujúci faktory, ktoré napomáhajú pri vytváraní reputačného skóre pre danú IP adresu. Na vytváranie reputačného systému budú potrebné externé zdroje, ako je znázornené na obrázku 1.. Externým zdrojom sa môže nazývať napríklad blacklist, ktorý je voľne dostupný na internete. Ďalším dôležitým faktorom pri tvorbe reputačného systému sú nástroje, ktoré budú obohacovať systém o funkcionalitu. Výstupom budú kompletné informácie o danej entite, reputačné skóre každej entity.

1.3 Prístupy k tvorbe reputácií sieťových entít

- Systéme NOTOS v práci [5] je novo vytvorený systém, ktorý mal ako prvý určovať dynamicky reputačný systém DNS. Skúmali jednotlivé názvy domén. Snažili sa vytvoriť up-to-date DNS informácie o vhodných ale aj nežiadúcich doménových menách. Využíva združovanie algoritmov modelovania siete a zón správania vhodných a nežiadúcich domén. Tieto algoritmy používajú na výpočet reputačného skóre pre doménu.

- V práci [2] sa snažia povedať o zdanlivo odlišných útokoch ako podobné sú. Teda čo ich spája. Následne analyzujú či takéto útoky nie sú z rovnakých lokálnych sieti. Ak sú, vytvárajú sa časti siete, o ktorých môžeme povedať, že je pravdepodobný útok. V práci [4] sa nadväzuje na túto, tým, že skúmajú agregácie takýchto štvrtí. Skúmajú ako pravdepodobné je, že každá IP adresa z takéhoto rozsahu je nežiadúca a snaží sa o útok.

Hlavné ciele práce možno zosumarizovať do nasledovných bodov:

(1) Analyzovať reputácie sieťových entít v manažmente bezpečnostných informácií a udalostí
(2) Analyzovať a porovnať prístupy k tvorbe reputácií sieťových entít.
(3) Navrhnúť a implementovať reputačný systém pre manažment bezpečnostných informácií a udalostí.

1.3.1 Blacklisty

Sieťoví operátori bežne spracúvajú protokoly o bezpečnosti, napríklad vytvárajú firewally a systémy na detekciu narušovania siete, s cieľom monitorovať a zabraňovať neoprávnenej návštevnosti do sieti.
Takéto protokoly o zabezpečovaní poskytujú významnú časť digitálnych dôkazov na vykonávanie forenznej analýzy. Na základe zistených údajov sa údaje zhromažďujú v blacklistoch. Napríklad návštevnosť pochádzajúca zo zdroja na blackliste môže byť zaznamenaná, ďalej analyzovaná alebo dokonca odsunutá na okraj siete. Medzi príklady blacklistov patria zoznamy IP a DNS adries, ktoré pomáhajú blokovať nežiaduci webový obsah, výrobcov nevyžiadanej pošty a stránky neoprávneného získavania údajov.

Verejne blacklisty: Väčšina prác používa pri svojich systémoch práve open-source blacklisty. Sú to zdroje tretích strán, ktoré sú voľne dostupné na internete. Nachádza sa v nich mnoho vhodných záznamom, ktoré sú pre systémy prospešné a tieto blacklisty sú zadarmo. Zvyčajne sa v týchto zátnamoch nachádzajú informácie o adresách, IP alebo DNS, ktoré boli pozorované pri vykonávaní škodlivých aktivít na internete.

- **CBL** – je zložený blacklist, obsahuje IP adresy, ktoré spĺňajú aspoň jednu zo skupín: spam, vírusy, DNSBL. Je veľmi kvalitný a spoľahlivý blacklist.
- **PSBL** – udržuje IP adresy, ktoré obsahujú nežiadúcu poštu
- **Dshield –** je komunitný systém, ktorý zdieľa logy z firewallu, logy sú získavané od odborníkov po celom svete. Tieto logy zverejňuje verejnosti bezplatne na internete aby vedeli o aktuálnych internetových útokoch
- **SSH Blacklist** – sleduje útoky SSH, približne 90 SSH útokov za deň

Používateľské blacklisty: Alternatívou k verejným open-source blacllistom sú zoznamy, ktoré sa môžu získavať prostredníctvom súkromných dohôd, napríklad u poskytovateľa internetových služieb, ktorí v svojich sieťach monitorujú škodlivé aktivity. Tento typ blacklistov je menej používaný v systémoch, pretože väčšinou sa v dohode nachádza aj poplatok používania týchto záznamom na určitú dobu.

- **Provider A** – je známy poskytovateľ hostovania v Holandsku, na základe dohody, nemôžu zverejniť meno ani viac informácii o tomto blackliste
- **University of Twente/EWI** – pomocou poskytovateľa A zistili IP adresy spamerov, ktorí napádali poštové servery na fakultách informatiky, matematiky a elektrotechniky
- **CAIS/RNP** – nachádza sa v Brazílii. Zisťujú škodlivé IP adresy zo svojho mail servera.
- **QNET** – je holandská spoločnosť, ktorá vyvíja nástroje na zabezpečenie sieti a poskytuje malware kontrolu svojím zákazníkom. Spoločnosť má 125 honeypotov umiestnených v Holandsku. Zahŕňa útoky SSH, MySQL a zraniteľnosť Windows.

1.3.2 Badhood blacklist

- Používajú 3 metódy :

1. porovnávanie 2 rôznych blacklistov a zisťovanie podobnosti medzi nimi. V metóde sa počíta **počet zdrojových BadHood, MIN, MAX a PRIEMER** škodlivých hostiteľov v BadHood**, odchýlka** škodlivých hostiteľov

Na výpočet použili softvérové prostredie.

2. Prienik / pretínanie BadHood:

Porovnávame či 2 rôzne blacklisty sú v rovnakom BadHoode. Ak nám vznikne prienik, znamená to, že časť blacklistov sa nachádza v rovnakom susedstve (Badhoode).

3. Ak sa nájdu v BadHoode útočníci, ktorý sa nachádzajú v rôznych blacklistoch, tak chceme zistiť, či využívajú rovnaký počet počítačov (intenzitu útokov)
   Využíva sa bodový diagram a delta analýza

2 Návrh riešenia

Základným stavebným kameňom nášho reputačného systému sú dáta, ktoré sa získavajú zo starších už nameraných záznamov. Dáta sú čerpané z našej fakulty, teda Prírodovedecká fakulta UPJŠ.

2.1 Navrhovaný prístup:

Základná vec pri navrhovaní prístupu je formálna definícia významu reputácie, reputačného systému a reputačného skóre. Ako uviedli v práci [3] slovo "reputácia" definuje spoločnú mienku, ktorú majú subjekty o objektoch. Je založená na spoločnom zdieľaní názorov o objekte, skúsenosti s nimi a doterajšom správaním sa objektu, resp. subjektu. Reputačné skóre je definované ako pravdepodobnosť, že subjekt bude vykonávať škodlivú činnosť v blízkej budúcnosti, na základe jeho správania v minulosti.

Reputačné skóre je založené na predpokladoch budúcich útokov. Preto je vhodné definovať prístup k predikcii.

Vstupom do algoritmu predikcie bude súhrn všetkých škodlivých udalostí za určité uplynulé obdobie. Môže byť dopĺňané rôznymi ďalšími vstupmi ako štatistika o možno riziku. V našej práci to budú rôzne vstupy ako krajina, mesto, systém, ktorý zisťuje či je uvedená IP adresa na niektorých zoznamoch blacklistov, či má statický alebo dynamicky priradenú IP adresu.

2.2 Ďalšie problémy

2.2.1 Časový rozsah zozbieraných dát

Jedným z problémov pri reputácií je časový úsek zozbieraných dát. Je potrebné si správne určiť veľkosť dát, ktorú chceme analyzovať aby ich nebolo veľa ale na druhej strane aby výsledok nebol skreslený nedostatkom dát a teda nepresného výsledného skóre.

2.2.2 Najdôležitejšie informácie

Aký druh škodlivej aktivity nás bude v práci zaujímať. Keďže informácií môže byť veľa, je nutné vybrať si najdôležitejšie informácie, ktoré nás budu zaujímať najviac.

2.2.3 Druhy útokov

Na ktoré útoky sa budeme zameriavať? Je nutné si presne špecifikovať útoky, pretože sa môže stať, že IP adresa je skúmaná na jeden druh útoku, ktorý nikdy nevykonávala. Preto môže byť jeho povestné skóre veľmi dobré no pritom môže škodiť v inom druhu útoku, ktorý my nezaznamenávame.

2.2.4 Staré informácie

Ak je IP adresa označená ako zlá, škodlivá, znamená to, že bola pravdepodobne súčasťou botnetu ale inak prítomna pri útoku. Teda bola zaznamenaná v zozname blacklistu. Následné tejto IP adrese bolo pridelené zlé hodnotenie. Avšak s pribúdajúcim časom od posledného útoku sa skóre IP adresy nezmenilo a stále má nízke hodnotenie. Daná IP adresa mohla byť za takýto čas pridelená aj inému počítaču, ktorý nevykonával žiadne útoky a má neprávom pridelené zlé hodnotenie.

Takto môže reputačný systém nadobudnúť určitú mieru neistoty ku všetkým údajom. Je ťažké určiť, ako sa IP adresy presne menia. Môže to závisieť aj na rôznych aspektoch, napríklad či ide o IP adresu ktorá je pridelená staticky alebo adresu, ktorá je pridelená dynamicky.

2.2.5 Neistota v informáciách

Už v predchádzajúcom bode sme sa dozvedeli problém s neistotou v dátach. Reputačný proces hodnotenia môže byť nepresný, nespoľahlivý alebo inak neistý ak sa nedodržia a neurčia presne definície.

2.2.6 Mapovanie IP adresy

Hlavným cieľom reputačnej databázy je získavať vedomosti o nebezpečnom hostiteľovi lenže nás systém pracuj s IP adresami nie s konkrétnymi hostiteľmi. Avšak sledovanie individuálnych hostiteľov je praktický nemožné, pretože sa môže jednať o zasahovanie do súkromia hostiteľa. Preto je lepšie rozpoznávať aspoň dynamické rozsahy adries a NAT. Tým aj upraviť ich bodovanie.

3 Predbežné výsledky

3.1 Testovacie prostredie

V rámci testovania je **klientska časť aplikácie** nasadená na testovacom serveri umiestnenom v rámci počítačovej siete ŠDaJ UPJŠ v Košiciach. Použité technológie vyžadujú moderný webový prehliadač s podporou jazykov **HTML5 a CSS3**. Samotná vizualizácia vyžaduje podporu SVG a povolený JavaScript v prehliadači. Ako také je testovanie vykonávané v prehliadači Google Chrome verzie 34. **Serverová časť** je tvorená PHP skriptami, ktoré komunikujú s MySQL databázou obsahujúcu testovacie dáta.

3.2 Potrebné technológie

V práci využívame rôzne technológie. Na programovanie v systéme používame programovací jazyk Python. Keďže získané informácie je potrebné niekam ukladať, rozhodli sme sa pre SQL databázu. Ako výstup budú informácie na webovej stránke, na ktorú budeme používať framework Bootstrap. Vytvorenie stánky sa bude realizovať cez javascript. V práci tiež využívame skenovanie otvorených portov, na prácu s portami nám bude slúžiť Nmap.

3.3 Implementácia systému

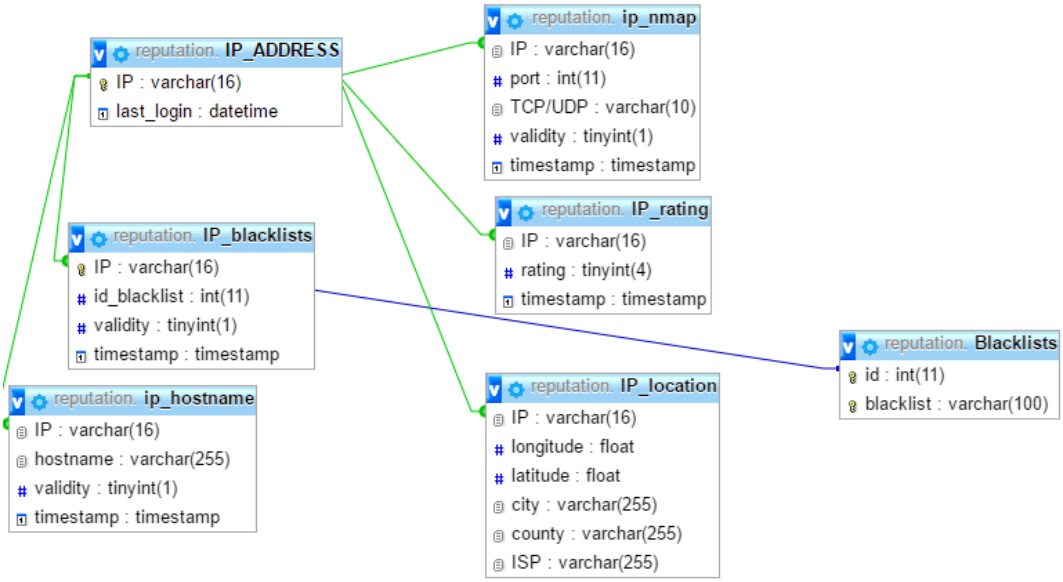
V tejto časti si predstavíme samotný návrh reputačného systému sieťových entít a implementáciu niektorých zásadných častí tohto systému. V predošlých kapitolách sme si predstavili základne pojmy, ktoré je potrebné vedieť k reputačným systémom. Taktiež sme sa oboznámili s pojmom blaclistov a sieťových entít, ktoré sa v systéme analyzujú.

Začali sme s analýzou údajov niekoľkých náhodne generovaných adries. Momentálne využívame na získavanie informácií o entitách (či už IP adresy, DNS adresy, email) voľne dostupný open-source systém Moocher.

Systém dokáže získavať informácie o IP adresách zo 45 rozsiahlych blacklistov. V týchto IP blacklistoch sa nachádza okolo 1 219 580 záznamov IP adries, ktoré sa nachádzajú v blacklistoch.

Rovnakým spôsobom vieme získavať informácie o DNS adresách zo 6 DNS blacklistov. V blacklistoch sa nachádza okolo 18 445 DNS záznamov.

Tým istým spôsobom získavame informácie o emailoch. Sú to informácie zo 6 mailových blacklistoch, kde sa nachádza približne 3 219 854 záznamov o spame.
Spolu tento systém uchováva informácie zo 63 blacklistov, či už sú to IP, DNS alebo emailové adresy.



Obrázok 2. Class diagram databázy

Vytvorili sme vlastnú databázu na uchovávanie dát o jednotlivých entitách. Ako môžete vidieť na obrázku 2 v databáze sa nachádzajú informácie o entite, posledné prihlásenie, všetky blacklisty, ktoré boli doteraz nájdené pri jednotlivých entitách. Entita je obohatená aj o informácie o lokalizácií, hostname a získané informácie

z nástroja Nmap. Taktiež ku každej entite existuje hodnotenie. Každá získaná informácia o entite ovplyvňuje výsledné hodnotenie entity. Niektoré informácie majú pri hodnotení vyššiu prioritu iné nižšiu. Po zozbieraní informácií je vypočítaný index danej entity.

5 Záver

V práci sme začali s analyzovaním externých zdrojov. Aké externé zdroje by sme mohli v našom systéme použiť. Následne sme skúmali konkrétne IP adresy v týchto vybratých externých zdrojoch. Skúmali sme v ktorých blacklistoch sa nachádzajú a aké najčastejšie útoky boli realizované. Tiež aj otvorené porty IP adresy a geografické údaje o IP adrese. Momentálne sa pracuje na základoch systému. Taktiež na analýze prístupov. V najbližšej budúcnosti nás čaká vytvorenie databázy na ukladanie informácií o IP adrese, implementácia systému a testovanie IP adries.

Poďakovanie Týmto by som chcela poďakovať vedúcemu svojej práce RNDr. JUDr. Pavlovi Sokolovi za trpezlivosť, cenné pripomienky a obetavosť počas tvorby bakalárskej práce.

Literatúra

[1] JACOBS, Jay; RUDIS, Bob. Data-Driven Security: Analysis, Visualization and Dashboards. John Wiley & Sons, 2014.

[2] MOURA, Giovane César. Internet bad neighborhoods. Giovane Cesar Moreira Moura, 2013.

[3] BARTOŠ, Václav; KOŘENEK, Jan. Evaluating Reputation of Internet Entities. In: IFIP International Conference on Autonomous Infrastructure, Management and Security. Springer International Publishing, 2016. p. 132-136.

[4] MOURA, Giovane CM, et al. Internet bad neighborhoods aggregation. In: 2012 IEEE Network Operations and Management Symposium. IEEE, 2012. p. 343-350.

[5] https://redmine.openinfosecfoundation.org/projects/suricata/wiki/IP_Reputation

[6] MISHSKY, Igor; GAL-OZ, Nurit; GUDES, Ehud. Computing domains reputation using flow. In: *Internet Technology and Secured Transactions (ICITST), 2014 9th International Conference for*. IEEE, 2014. p. 426-431.

[7] ANTONAKAKIS, Manos, et al. Building a Dynamic Reputation System for DNS. In: *USENIX security symposium*. 2010. p. 273-290.