UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA
PRÍRODOVEDECKÁ FAKULTA

IDENTIFIKÁCIA TYPOV ÚTOČNÍKOV POMOCOU ÚDAJOV Z HONEYPOTOV

DIPLOMOVÁ PRÁCA

Študijný program:	Informatika
Pracovisko (katedra/ústav):	Ústav informatiky
Vedúci diplomovej práce:	RNDr. JUDr. Pavol Sokol, PhD.

Košice 2017

Bc. Lenka KLEINOVÁ

1 Obsah

2 Aktuálne prístupy k identifikácii typov útočníkov

Jednou z úloh sietí je zabezpečiť anonymitu odosielateľa, príjemcu alebo oboch. Dosiahnutie stavu anonymity implikuje, že v sieti nie je žiaden útočník alebo útočník nie je úspešný pri svojich pokusoch o útok. To, či útočník bude alebo nebude úspešný pri svojej činnosti, sa zisťuje na základe bezpečnostnej evaulácie alebo analýzy rizík. Najkritickejšou časťou je určenie správneho modelu útočníka. Ak je tento model príliš silný, tak väčšina techník na ochranu nebude fungovať, naopak, ak je model útočníka príliš slabý, systém nebude poskytovať dostatočnú ochranu používateľov.

Talianski autori [1] sa vo svojom článku venujú modelovaniu útočníkovho správania pomocou grafov a Markovových rozhodovacích procesov na predikciu možných rozhodnutí útočníka. Zároveň predpokladajú, že útočník nemá presné a detailné informácie o systéme, na ktorý útočí, čo ho zaraďuje do kategórie tzv. **adaptívnych útočníkov.** Na rozdiel od **deterministických útočníkov**, ktorí systém dobre poznajú a majú dopredu naplánované kroky útoku, adaptívny útočník môže prehodnocovať a meniť svoje rozhodnutia v rámci útoku v závislosti od vzniknutých situácií. Deterministickí útočníci sa v každom okamihu útoku dokážu rozhodnúť, aký bude nasledujúci krok s cieľom dosiahnuť optimálnu cestu v grafe útoku. Graf útoku je podľa autorov článku popísaný nasledovne: Uzol S_i reprezentuje úspešne napadnutú zraniteľnosť, hrana medzi dvoma uzlami určuje možné využitie ďalšej zraniteľnosti a takéto postupné využívanie zraniteľností vedie k novým stavom v systéme a novým možnostiam pre útočníka.

Podľa článku z roku 2005 [2] je dôležité odhaliť riziká na základe vektorov útokov. Jedným zo spôsobov, ako predchádzať bezpečnostným incidentom je zistiť, ktoré typy útočníkov sú pre systém najnebezpečnejšie a zamerať sa na ochranu aktív, ktoré s veľkou pravdepodobnosťou títo útočníci napadnú. Autori vytvorili klasifikáciu útočníkov podľa ich záujmov a cieľov. Podľa daného článku a článku z roku 2003 [3] vieme útočníkov rozdeliť na skupiny a následne ich ohodnotiť podľa toho, aké riziko pre systém predstavujú. Ide o skupiny: **neštruktúrovaný hacker, štruktúrovaný hacker, organizovaný zločinec a priemyselná e-špionáž, insider, hacktivista, financovaná teroristická skupina, štát, skript kiddie, „hobby“ hacker.** Výsledné ohodnotenie útočníka závisí od viacerých aspektov. Od jeho technických zručností, od zdrojov, ktoré ma k dispozícii, od jeho zámeru a motivácie, a od pravdepodobnosti,

s akou je systém napadnuteľný daným typom útočníka. V článku autori odvodili vzťah na číselné ohodnotenie toho, aké riziko daný útočník predstavuje a na číselné ohodnotenie jeho schopností. Podľa týchto hodnotení je potrebné nasadiť príslušné opatrenia proti danému útočníkovi.

V ďalšej práci sa autori [4] zaoberajú profiláciou útočníkov ako koncept oddelenia vlastností infraštruktúry systému od vlastností útočníkov. V článku autori ukazujú, ako je možné poznatky o profilácii útočníka integrovať do existujúcich bezpečnostných nástrojov bez akejkoľvek ujmy na výkonnosti. Ako príklad takejto integrácie uvádzajú analytický nástroj AproxTree+, ktorý je rozšírením existujúceho nástroja AproxTree. Pri analýze využívajú stromovú štruktúru na reprezentáciu útoku, ktorá predstavuje hierarchický popis možných útokov proti cieľovej infraštruktúre. V strome sú pokryté všetky možné scenáre útoku. Berúc do úvahy profiláciu útočníka, je možné prechádzaním stromu vylúčiť určité uzly, a tým celé podstromy a naopak identifikovať tie scenáre, ktoré pri danom type útočníka ohrozujú konkrétny systém. V závislosti od množstva a detailnosti informácií, ktoré sú o útočníkovi k dispozícii, je scenár vymedzený užšie a je ho tak možné ľahšie analyzovať.

Autori v nasledujúcom článku [5] priniesli ďalší pohľad na klasifikáciu útočníkov. V práci autori navrhli novú metódu charakterizácie útočníkov, ktorá je menej abstraktná ako v niektorých iných riešeniach a viac praktická a realistická. Autori predpokladajú, že útočník pozná infraštruktúru siete a jej algoritmy, keďže väčšina implementácií je open-sourcová a dobre zdokumentovaná. Vytvorili delenie útočníkov ako entít zúčastňujúcich sa nejakým spôsobom transakcií medzi dvoma stranami využívajúc anonymnú sieť. Trieda **externých strán** je považovaná za najslabšieho útočníka, jeho vplyv je limitovaný keďže nemá žiadnu kontrolu nad počítačom medzi dvoma komunikujúcimi stranami. **Poskytovateľ služby** je trieda predstavujúca komunikačného partnera používateľa, je zviazaný s komunikujúcimi stranami, čo je možné ľahko zneužiť. Útočníci patriaci do triedy **lokálnej administrácie** môžu manipulovať so všetkým v blízkosti používateľa, čo je nebezbečné najmä vtedy, keď používateľ slepo dôveruje všetkým prenášaným údajom. Ďalším silným útočníkom je **poskytovateľ internetového pripojenia,** keďže má prístup k veľkému počtu počítačov. Čiže je možné, že väčšina dátového toku medzi dvoma komunikujúcimi stranami je zachytávaná týmto typom útočníka. **Vláda** je ďalším typom nebezpečného útočníka pretože má prístup k významnej časti sietí, má zdroje na vytváranie falošných služieb,

zdroje na prelomenie jednoduchších šifrovacích schém alebo zdroje na zakázanie prístupu k špecifickým službám. **Tajné služby** tvoria najvyššiu triedu útočníkov. Môžu získať prístup k väčšine častí globálnych sietí, ak je to nevyhnutné pre ich operáciu. Okrem toho, nepodliehajú žiadnemu typu zákona, čo z nich robí vážnu bezpečnostnú hrozbu.

V práci [6] sa autori zameriavajú na motiváciu útočníka. Navrhli framework, ktorý zahŕňa motiváciu útočníka v analýze útoku pomocou stromu útoku. Rozlišujú 5 typov motivácií útočníka: **finančný zisk, spôsobenie škody, získanie znalosti, vyhľadávanie zábavy, získanie notoričnosti v rámci komunity.** Ďalší krok v určovaní profilu útočníka je určenie zdrojov, ktorými útočník disponuje. Do úvahy autori berú hodnoty nasledovných parametrov: **financie**, ktoré má útočník k dispozícii; **schopnosti** útočníka; **čas,** ktorý má útočník k dispozícii na vykonanie útoku. Po nastavení stromu útoku a profilu útočníka sa tieto dva aspekty skombinujú a vykoná sa analýza, ktorá vedie k presnejšiemu typu útočníka.

Existujú mnohé ďalšie klasifikácie, napríklad v [7] nájdeme 4 typy útočníkov: **eavesdropper, global eavesdropper, pasívny a aktívny nepriateľ.** Problém s týmto delením je však ten, že v praxi je medzi týmito kategóriami veľmi malý rozdiel a je ťažké presne začleniť útočníka do niektorej z nich.

Systematické rozdelenie útočníkov pre teoretické modelovanie je popísané v [8]. Podľa toho, či je útočník v sieti alebo nie, rozlišujeme **interných a externých** útočníkov. Podľa toho, či útočník môže zmeniť stav siete alebo nie rozlišujeme **pasívnych a aktívnych** útočníkov a podľa toho, či útočník môže meniť svoje zdroje a vyvíjať svoje schopnosti počas útok alebo nie, rozlišujeme **statických a adaptívnych** útočníkov.

3 Honeypoty

3.1 Definícia honeypotu

Honeypot môže byť definovaný viacerými spôsobmi. Jedna z definícií hovorí, že honeypot je program, ktorý na prvý pohľad vyzerá ako atraktívna služba, či skupina služieb, celý operačný systém alebo dokonca celá počítačová sieť, no v skutočnosti ide len o systém, ktorého úlohou je nalákať útočníka a monitorovať jeho činnosť[9]. Honeypot teda monitoruje a zaznamenáva každý krok, ktorý útočník urobí, čo zahŕňa pokusy o prístup do systému, všetky stlačené klávesy klávesnice, súbory, ku ktorým sa pristúpilo a ktoré boli modifikované a vykonané procesy. Lance Spitzner, zakladateľ Honeynet Project-u, definuje honeypot nasledovne: „Honeypot je informačný systém, ktorého hodnota spočíva v jeho neautorizovanom alebo nedovolenom využití.“ [10] Na honeypote je spustený emulovaný operačný systém a služby, ktoré sa správajú ako „pasca“ a ich úlohou je nalákať útočníka, aby zneužil systém na nejakú nekalú činnosť, pričom v skutočnosti honeypot len zaznamenáva všetky prostriedky, ktoré útočník na túto činnosť využíva[9].

3.1.1 Generický model honeypotu

Honeypot je umiestnený do siete s jediným účelom, a to byť napadnutý. Je navrhnutý s úmyselnými nechránenými miestami, ktoré sú odhalené vo verejnej sieti. Honeypot nemá žiadnu produkčnú hodnotu a každý prístup k nemu je považovaný za nelegálny. Honeypot obsahuje:[9]

- Produkčný systém honeypotu- nejde o skutočný produkčný systém, len o akúsi „korisť“ pre útočníka. Poskytuje honey (med), teda súbory a falošné systémové prostriedky a na každú útočníkovu aktivitu je nastavená automatická odpoveď, aby honeypot vyzeral ako skutočný produkčný systém.

- Firewall- poskytuje záznamy o tom, ako sa útočník pokúsil dostať do systému honeypotu. Zaznamenáva všetky pakety idúce do systému, pretože každý prístup do honeypotu má nejaký nelegálny dôvod.

- Monitorovacia jednotka- ide o jednotku vyhodnocujúcu ohrozenie, ktorá monitoruje aktivity v sieti a/alebo v systéme a zisťuje tak škodlivú činnosť. O každej takejto činnosti informuje riadiacu stanicu. Prehodnocuje poradie, časové pečiatky a typ paketov, ktoré útočník použil na získanie prístupu do honeypotu a stlačené klávesy či

zmenené súbory pomáhajú identifikovať prostriedky, metodiku a zámery útočníka. Ako monitorovacia jednotka môže slúžiť systém na detekciu útoku (intrusion detection system-IDS).

- Výstražná jednotka- Honeypot by mal byť schopný generovať upozornenie, výstrahu cez email a poslať administrátorovi upozornenie o toku údajov z alebo do honeypotu. Tak môže administrátor skúmať útočníkovu aktivitu ešte počas doby, keď prebieha.

- Zaznamenávacia jednotka- poskytuje efektívne uchovanie všetkých systémových záznamov, záznamov firewallu a záznamov o toku údajov medzi firewallom a honeypotom.

3.2 Výhody a nevýhody honeypotov

V oblasti bezpečnosti majú honeypoty od svojho vzniku postavenie úspešného nástroja a technológie využívanej v spojení s Intrusion Detection System (IDS) a firewallmi. Napriek mnohým výhodám, honeypot ako mechanizmus včasnej detekcie podozrivej činnosti v sieti so sebou prináša aj riziká, a to najmä riziko útoku v sieti, do ktorej je honeypot nasadený. Medzi dôležité výhody honeypotov patrí:[9]

1) Údaje zbierajú len vtedy, keď niekto alebo niečo s nimi interaguje. To robí údaje, ktoré honeypot zbiera jednoduchšie na spracovanie a analýzu.

2) Honeypoty výrazne redukujú počet falošných výstrah. Akákoľvek aktivita s honeypotom je z jeho definície neautorizovaná, čo robí detekciu útokov omnoho efektívnejšiu. Honeypoty nemajú žiadnu produkčnú hodnotu a nikdy by nemali byť použité nikým iným ako administrátorom. Každý tok údajov do honeypotu okrem očakávaného administratívneho toku je pravdepodobne škodlivý. Každý tok údajov z honeypotu je škodlivý. Preto sa v údajoch nebude nachádzať žiaden, resp. veľmi malý šum a preto by všetko, čo honeypot zachytí, malo byť analyzované. Tento nízky počet falošných výstrah je oproti IDS alebo firewallu veľkou výhodou honeypotov. Vďaka tomu je možná rýchla detekcia hrozieb a generovanie upozornenia.

3) Keďže každé pripojenie na honeypot je považované za hrozbu, tak dosiaľ nepoznané útoky sú odhalené tak rýchlo ako aj tie, ktoré sú už známe. Hovoríme o takzvaných „zero-day“ hrozbách, ktoré sú odhaľované vďaka honeypotom. Honeypoty dokážu zachytiť všetko týkajúce sa útočníka, čo zahŕňa sieťové pakety, uploadovaný

malware, všetku komunikáciu cez chat a všetky príkazy. Tak vie administrátor zistiť, čo útočník robí a ako to robí.

4) Ďalšou výhodou je jednoduchosť. Neexistujú tu žiadne špeciálne algoritmy, ktoré by bolo treba vyvíjať, netreba udržiavať žiadne stavové tabuľky, ani obnovovať podpisy kvôli šifrovaniu. Vyžadujú minimálne prostriedky, dokonca i vo veľmi veľkých počítačových sieťach.

5) Na rozdiel od mnohých iných bezpečnostných technológií, ako je napríklad IDS, honeypoty dokážu fungovať aj v šifrovanom alebo v IPv6 prostredí. Preto nezáleží na tom, čím útočník zaútočí, honeypot to zachytí.

Rôzne typy honeypotov so sebou prinášajú rôzne riziká. Medzi ne patria aj nasledovné: [9]

1) Pokiaľ na honeypoty nik neútočí, sú zbytočné.

2) Honeypoty vidia len to, čo je namierené priamo na ne. To znamená, že ak sa útočník dostane do siete a zaútočí na systémy v nej okrem daného honeypotu, tento honeypot nebude vedieť nič o útočníkovej aktivite pokiaľ nie je útok namierený práve naň. Okrem toho, ak útočník identifikuje honeypot, t.j. zistí, že nejde o skutočný produkčný systém, môže sa honeypotu úspešne vyhýbať a napadnúť organizáciu bez toho, aby o tom honeypot vedel.

3) Útočník môže využiť honeypot aj vo svoj prospech. Ak úspešne vnikne do tohto systému, môže ho ďalej využívať na ďalšie útoky (zneužitie honeypotu).

4) Ďalším rizikom honeypotov je takzvaný fingerprinting. Ide o to, že útočník vie identifikovať, že ide o honeypot, pretože systém, o ktorom si útočník myslí, že je produkčný, má určité očakávané charakteristiky alebo správanie, ktoré honeypot v dôsledku zlého nastavenia nemá.

5) Fingerprinting je veľkou hrozbou najmä pre výskumné honeypoty. Po tom, čo útočník odhalí, že ide o honeypot, môže zásobovať daný honeypot zlými, zavádzajúcimi informáciami, čím privedie výskumný bezpečnostný tím k nesprávnym záverom.

Kvôli týmto nevýhodám honeypoty nemôžu úplne nahradiť iné bezpečnostné systémy. Napriek tomu však týmto systémom pridávajú hodnotu a robia ich účinnejšími.

4 Prehľad existujúcich honeypotov

Rôzne typy honeypotov umožňujú zberať rôzne údaje o útoku, resp. o útočníkovi, ktorý za konkrétnym útokom stojí. Vyše 60% všetkých útokov sú práve útoky namierené proti webovým aplikáciám. Cieľom týchto útokov sú väčšinou stránky organizácií prostredníctvom ktorých je potom zákazníkom sprostredkovaný škodlivý obsah alebo je spôsobený únik citlivých informácií. Na lepšie pochopenie týchto útokov a ochranu webových aplikácií tu sú webové honeypoty.

Technologický pokrok zmenil spôsob komunikácie a interakcie medzi používateľmi. Web sa stal miestom zdieľania informácií a prostriedkom pre rôzne komerčné transakcie. Je možné tu nájsť informácie z veľkého množstva zdrojov z celého sveta. Spolu so všetkými výhodami webu sa však objavila aj hrozba útokov. Komplexnosť webu a rôzne bezpečnostné diery v infraštruktúre robia web zraniteľným voči útokom ohrozujúcich koncových používateľov po celom svete. Medzi najčastejšie škodlivé aktivity na webe patrí zvyšovanie počtu „drive-by“ sťahovaní z rôznych webových stránok, útoky sú dobre maskované a dynamicky sa vyvíjajú, čím sa antivírusové programy stávajú pre ne úplne neefektívne, útoky sú namierené voči pluginom prehliadača, zvyšuje sa množstvo škodlivých aplikácií, napadnutie SQL databáz ohrozuje dáta rôznych web stránok, používatelia sú presmerovávaní na škodlivé webové stránky prostredníctvom takzvaných „malvertisementov“ atď.

V súčasnosti môže byť akákoľvek webová stránka napadnutá útočníkom a použitá na útok namierený proti akémukoľvek počítaču. Existujú techniky na napadnutie počítača koncového užívateľa počas jeho prezerania webových stránok pričom tradičné prístupy k ochrane, ako napríklad antivírusové programy, sa stávajú neužitočnými. [11]

V tejto kapitole sa zameriavame na 6 existujúcich honeypotov a údaje, ktoré zberajú.

4.1 Glastopf

Glastopf je minimalistický nízko-interaktívny webový honeypot napísaný v Pythone, ktorý je navrhnutý na zachytávanie informácií o aktuálnych útokoch na webové aplikácie, ako sú napríklad SQL Injection, remote file inclusion a local file inclusion útoky. Emuluje tisícky zraniteľností. Glastopf skenuje prichádzajúce

požiadavky a hľadá najmä reťazce ako „=http://“ alebo „CAST(0x“. V prípade, že sa nájde zhoda, stiahne sa súbor, analyzuje sa a Glastopf odpovie útočníkovi tak, aby to bolo čo najbližšie jeho očakávaniam. Ak splní útočníkove požiadavky, útočník poskytne ďalšie pre nás užitočné údaje.

Údaje, ktoré vieme získať o útoku s využitím honeypotu Glastopf sú: TIME, SOURCE, REQUEST_URL, REQUEST_RAW, PATTERN, FILENAME, COUNT, FIRSTTIME, LASTTIME, CONTENT.

4.2 Kippo

Kippo je stredne-interaktívny SSH honeypot, ktorý je navrhnutý na zaznamenávanie brute force útokov a celej shell interakcie útočníka so systémom. Rovnako ako Glastopf je napísaný v Pythone. Umožňuje pridávať falošný obsah do súborov, čiže útočník môže prečítať súbory ako napríklad /etc/passwd s falošným obsahom. Kippo počúva ssh spojenia na porte 2222, pričom port je možné zmeniť.

Údaje, ktoré vieme získať o útoku pomocou honeypotu Kippo sú: SESSION, SUCCESS, USERNAME, PASSWORD, TIMESTAMP, IP, STARTTIME, ENDTIME, CLIENT, SENSOR, URL, OUTFILE.

4.3 Dionaea

Dionaea je nízko-interaktívny honeypot zameraný na zachytávanie malvéru. Je rovnako ako predchádzajúce dva honeypoty napísaný v Pythone.

Údaje, ktoré môžeme získať o útoku pomocou tohto honeypotu sú: CONNECTION, CONNECTION_TYPE, CONNECTION_TRANSPORT, CONNECTION_PROTOCOL, CONNECTION_TIMESTAMP, CONNECTION_ROOT, CONNECTION_PARENT, LOCAL_HOST, LOCAL_PORT, REMOTE_HOST, REMOTE_HOSTNAME, REMOTE_PORT.

4.4 Honeyware

Honeyware je nízko-interaktívny klientský honeypot, ktorý kombinuje výhody webových nástrojov, ktoré bežia na lokálnych alebo vzdialených serveroch so schopnosťou pristúpiť k nástrojom cez webový prehliadač. Umožňuje testovať cieľový webový server pomocou takmer všetkých webových prehliadačov a skenovať cieľ pomocou piatich skenovacích nástrojov. Je napísaný v PHP a je to open sourcový nástroj. Jeho základné vlastnosti sú: dokáže simulovať webové prehliadače ako Internet

Explorer, Firefox, Opera, Chrome, Safari. Dokáže skenovať cieľové súbory, aby určil či ide o škodlivý kód alebo nie, ďalej poskytuje nástroje na hľadanie URL, ktoré je potrebné skenovať. Je tu tiež implementovaný klientský nástroj, ktorý interaguje s cieľovým servrom kvôli kontrole súborov stiahnutých na honeyware.

Čo sa týka architektúry, tak používateľ si môže vybrať aký webový prehliadač má honeyware simulovať. Výhodou tohto je to, že niektorí útočníci využívajú nástroj Mpack a útočia len na tých návštevníkov, ktorí využívajú nejaký konkrétny prehliadač, teda napríklad prehliadač s istou zraniteľnosťou. Každý webový prehliadač používa tzv. user agent čo je reťazec poslaný cieľovému servru. Tento user agent obsahuje informácie o názve, verzii browsera a tiež o OS hosta. Vďaka tomu je možné simulovať browser honeywarom. Čiže po detegovaní browsera je možné presmerovať používateľa na konkrétny exploit, ktorý je namierený proti nejakému systému. Samozrejme umožňuje ukladať skeny a výsledky crawlingu do databázy.

4.5 DShield

Cieľom honeypotu DShield je zber kvantitatívnych dát a zisťovanie aktivity automatických a poloautomatických snímačov webových aplikácií. Honeypot pozostáva z 3 častí: klient, súbor templejtov a logovací systém. Všetky requesty na honeypot idú na klienta, ktorý porovnáva požadovanú webovú aplikáciu s nainštalovanými templejtmi. Ak sa nájde vhodný templejt tak sa pošle útočníkovi. Ak nie, tak sa mu zobrazí defaultná webová stránka. V oboch prípadoch sa request zaznamená do centrálnej DShield databázy. V súčasnosti tento webový honeypot beží na Windowsoch, Linuxoch aj na Mac OSX.

4.6 HIHAT

HIHAT teda High Interaction Honeypot Analysis Toolkit umožňuje transformovať ľubovoľnú PHP aplikáciu na webový vysoko-interaktívny honeypot. Vďaka používateľskému rozhraniu je možné monitorovať honeypot a analyzovať potrebné dáta. Príkladom je transformácia PHPMyAdminu na plne funkčný honeypot, ktorý poskytuje všetky funkcionality no navyše v pozadí zaznamenáva a monitoruje všetko dianie. Tento honeypot má množstvo vlastností ako napríklad skenovanie za účelom identifikácie už známych útokov, umožňuje detekovať napríklad pokusy o stiahnutie škodlivých súborov pomocou príkazov ako WGET alebo CURL. Poskytuje detailné informácie o prístupe k honeypotu , najmä http-GET, http-POST a COOKIE

dáta. Kópie škodlivých nástrojov ukladá na bezpečné miesto pre ďalšiu analýzu. Poskytuje množstvo štatistík a generuje mapy zobrazujúce odkiaľ útoky prichádzajú.

5 Klasifikácia útočníkov

Predtým než prejdeme k jednotlivým skupinám útočníkov, pozrime sa na niektoré dôležité trendy v oblasti hrozieb, ktoré majú vplyv na aktivity útočníkov.

Realitou v súčasnosti je fakt, že služby kybernetickej kriminality sú lacné. Ceny za krádež dát a za iné služby podobného charakteru stále klesajú. Práve útočníci sú v pozícii, v ktorej majú na nízke ceny najväčší vplyv, čo zvyšuje riziko a počet útokov.

Jednotlivci majú motiváciu vykonávať útoky najmä kvôli nedostatočnému zabezpečeniu systémov, vďaka ktorému môžu aj nováčikovia vykonať úspešný SQL Injection útok alebo phishing útok.

Dark web a dark net je využívaný ako akási skrýša pre útočníkov, ktorí ho vedia zneužiť vo svoj prospech. Prístup k nim vyžaduje určité technické znalosti a na jeho zabezpečenie pred neželanými „návštevníkmi“ boli implementované rôzne technické prekážky.

Útočníkov v kyberpriestore je veľmi náročné identifikovať a nájsť. Čiže len veľmi málo z nich si za svoje činy odpykáva trest. To je ďalší dôvod rozmáhania sa práve takéhoto typu útokov.

Ak sa bavíme o skupinách útočníkov, tak sa zameriavame na ich motivácie a schopnosti, pričom keď rozprávame o útokoch, tak nás zaujímajú nástroje a metódy, ktoré útočníci využívajú. My sa v nasledujúcom budeme zameriavať práve na motivácie a schopnosti útočníkov.

Podľa štatistík z roku 2015 je najviac útočníkov zaradených do skupín kyberkriminálnici, insideri, kyberšpióni a cyber warriors. [12]

Cyber-criminals

Ich hlavnou motiváciu je speňaženie poskytovaných služieb. Pracujú na zlepšovaní využívaných infraštruktúr aj na vyvíjaní stále sofistikovanejších škodlivých nástrojov. [12]

Insiders (zamestnanci)

Táto skupina útočníkov je v súčasnosti pomerne dobre rozanalyzovaná a je vytvorená detailnejšia klasifikácia tohto typu útočníkov. Ide o skupinu súčasných a bývalých zamestnancov, súčasných a bývalých poskytovateľov/dodávateľov/konzultantov, súčasných a bývalých obchodných

partnerov a zákazníkov. Okrem speňaženia a istého druhu pomsty, je u nich najväčšou motiváciou zneužitie prístupových práv. Ukázalo sa, že najčastejšie zneužívané prístupové údaje sú údaje koncových používateľov, zákazníkov, finančníkov a vedúcich pracovníkov. Systémoví administrátori sú až na 9tom mieste. Často krát majú útočníci z inej skupiny záujem využiť insiderov na dosiahnutie vlastného cieľa. Pričom najčastejší spôsob, ako ich získať je podplatenie. Súčasné informácie o tejto kategórii boli získané pomocou modelovania a tiež pomocou reakčnej analýzy. [12]

Online social hackers

Počet týchto útočníkov sa zvyšuje vďaka phishingovým útokom, ktoré sú zamerané vždy na konkrétne skupiny obetí. Na získanie informácií o tejto skupine sú dôležité informácie od poskytovateľov sociálnych sietí. Nástroje pre tento typ útokov sú ľahko dostupné, takže jednotlivcom s nejakou konkrétnou motiváciou nestojí nič v ceste. Informácie o nich sú získavané na základe reakčnej analýzy, t.j. na základe analýzy konkrétnych bezpečnostných incidentov. [12]

Hacktivists

Ich hlavným cieľom je šíriť informácie organizácií alebo vplyvných ľudí s cieľom zahanbiť ich a zvýšiť informovanosť verejnosti o tom, čo robia ilegálne. Propagujú slobodu vyjadrovania a otvorenosť internetu. Často majú tieto skupiny rovnaké ciele ako bezpečnostné spoločnosti a preto by bolo spojenie týchto dvoch skupín zaujímavým riešením rôznych konfliktov. [12]

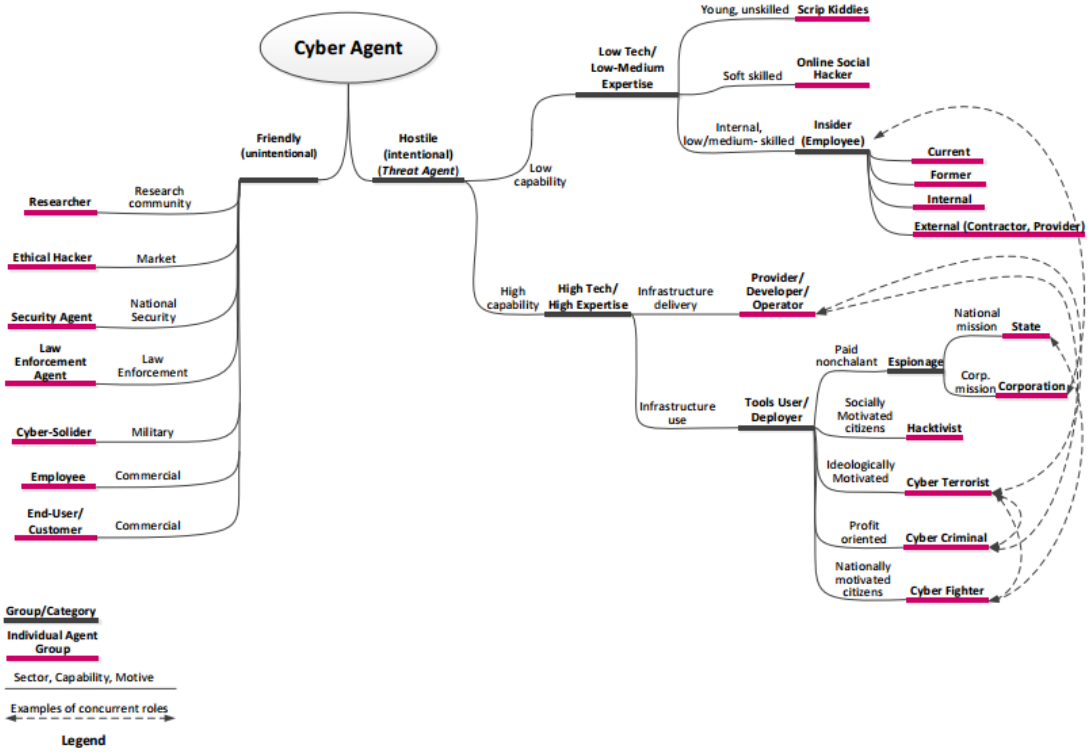
Cyber-terrorists

Moderné technológie internetu sa stali komunikačným kanálom a kanálom na verbovanie nových členov tejto skupiny útočníkov. Využívajú pritom útočníkov klasifikovaných ako social online hackers na udržiavanie ich infraštruktúry a na šírenie ich kampane po sociálnych sieťach. Aj ich záujmom sú finančné transakcie. [12]

Script kiddies

Na internete sa nachádza množstvo informácii k tomu, aby bolo možné vykonať útok alebo vytvoriť vlastný malware. Vďaka tomu rastie počet účasti tejto skupiny na rôznych bezpečnostných incidentoch. Niektorí z týchto útočníkov nemajú žiaden vážny zámer a vykonávajú túto činnosť len pre zábavu. Často krát ani nevedia, čo svojim útokom spôsobia. Za posledné obdobie sa ukázalo, že za týmito útokmi stoja najmä teenageri. [12]

Na nasledujúcom obrázku je zhrnutá celá klasifikácia útočníkov.



Nasledujúca tabuľka zobrazuje, ktoré typy útočníkov sú pôvodcami ktorých útokov.

	Threat Agents								
	Cyber criminals	Insiders	Online social hackers	Nation States	Corporations	Hacktivists	Cyber Fighters	Cyber terrorists	Script kiddies
Malware	✓	✓	✓	✓	✓	✓	✓	✓	✓
Web-based attacks	✓			✓	✓	✓	✓	✓	✓
Web application attacks	✓			✓	✓	✓	✓	✓	✓
Botnets	✓			✓	✓	✓	✓	✓	✓
Denial of service	✓			✓	✓	✓	✓	✓	✓
Physical damage/ theft /loss	✓	✓		✓	✓			✓	
Insider threat	✓	✓		✓	✓			✓	
Phishing	✓	✓	✓	✓	✓	✓	✓	✓	✓
Spam	✓		✓	✓	✓	✓	✓	✓	✓
Exploit kits	✓			✓	✓	✓			✓
Data breaches	✓	✓		✓	✓	✓	✓	✓	✓

Vektor útoku

Každý útok pozostáva z konkrétnych krokov, ktoré útočník vykonal. Táto postupnosť krokov sa nazýva vektor útoku. Niektoré vektory môžu pozostávať aj z viacerých hrozieb a naopak niektoré kroky, ktoré útočník vykonal nemusia byť škodlivé. Každý krok môže zahŕňať objekt, na ktorý útočník útočí, jeho zraniteľnosti, nástroj, pomocou ktorého je možné túto zraniteľnosť využiť a presunúť sa na ďalší objekt, čo napokon vytvára úspešný útok. Znalosť vektora útoku je veľmi dôležitá kvôli správnemu pochopeniu detailov útoku a lepšej obrane proti ďalším útokom. [12]

Na to, aby sme lepšie pochopili taktiky útokov vo všeobecnosti a vedeli, ako sa proti nim brániť, sa pozrieme na 3 typy útokov: útoky proti cyber-physical systémom, APT útoky, cielené útoky.

Útoky proti CPS

CPS alebo „smart system“ je systém spolupracujúcich výpočtových jednotiek kontrolujúcich fyzické entity. Väčšinou sú navrhnuté ako sieť interagujúcich prvkov. Patria sem najmä systémy pre priemyselnú výrobu, na ktoré majú útoky veľmi škodlivý dopad. Tento typ útoku musí najprv odhaliť zraniteľnosti všetkých komponentov systému, ktoré môžu byť softvérové, hardvérové ale aj také, ktoré súvisia s ľudským faktorom. V závislosti od zraniteľnosti väčšinou nasleduje cielený phishing. Ako náhle je systém napadnutý a malware nainštalovaný, útočník vytvorí komunikačný kanál a môže riadiť a kontrolovať systém. Charakteristickou črtou týchto útokov je priamy dosah na zariadenia fyzického sveta. Na ich vykonanie je však často potrebná znalosť konkrétneho systému najmä pri SCADA systémoch. Za týmito útokmi sú väčšinou útočníci zo skupiny cyber teroristov, cyber kriminálnikov alebo hacktivistov. [12]

Cielené útoky

Ide o útoky namierené proti konkrétnemu jednotlivcovi, spoločnosti, systému alebo softvéru s využitím konkrétnych poznatkov o cieli. Tieto útoky nie sú až tak rozšírené. Na základe poznatkov a cieli, útočník pošle špecifické správy s cieľom nalákať obeť, s tým, že tieto falošné správy sa nedajú odlíšiť od skutočných. V inicializačnej fáze, keď útočník zbiera informácie o systéme, sa zameriava na IT prostredie, infraštruktúru systému ale aj na informácie o jednotlivých osobách. Po získaní prístupu sa využije zraniteľnosť na vykonanie škodlivého kódu. Väčšinou ide o stiahnutie malwaru do systému koncového používateľa, ktorý vytvorí komunikačný

kanál s útočníkom, ktorý následne môže vykonávať rôzne akcie (napríklad získavať informácie o spoločnosti). Časté metódy využívané pri tomto typu útoku sú phishing email, zero day útoky, ale útočníci tiež využívajú sociálne siete k tomu, aby čo najviac používateľov kliklo na link a stiahlo malware. Súčasťou cielených útokov môžu byť všetky skupiny útočníkov. [12]

Advanced Persistent Threats (pokročilé dlhotrvajúce hrozby)

Ide o rozmanitú množinu utajených procesov namierených proti špecifickým objektom. Sú väčšinou vykonávané v rámci kampaní proti konkrétnym organizáciám. Hlavným cieľom je získanie dát a nie poškodenie siete. Úspešný útok tohto typu vyžaduje utajenosť počas celej dĺžky trvania útoku. Tí, ktorí stoja za týmto typom útoku majú väčšinou pokročilé znalosti, všetko dopredu plánujú, využívajú špeciálne vytvorené malwary a detailné poznatky o obeti. Útočníci väčšinou disponujú rozsiahlymi zdrojmi a finančnými prostriedkami. Cieľom je umiestniť vytvorený škodlivý kód na jeden alebo viac počítačov a vykonávať ho pre dosiahnutie konkrétneho cieľa, čo najdlhšiu dobu. Ide o útoky, ktoré sú cielené, útočníci majú splniť nejakú misiu, ktorá je organizovaná, dobre finančne zabezpečená a silno motivovaná. Hlavným znakom je dlhé trvanie útoku. Sú tiež podporované externe kyberkriminálnikmi, hacktivistami či dokonca špecializovanými spoločnosťami. [12]

5.1 Vlastnosti útočníka

Na zaradenie útočníka do skupiny budeme uvažovať 3 jeho vlastnosti:

Schopnosti útočníka- pod schopnosťami útočníka budeme rozumieť jeho schopnosti v oblasti počítačovej kriminality, resp. jeho skúsenosti s napadnutím systému.

Znalosti útočníka- pod znalosťami útočníka rozumieme to, do akej miery pozná systém, resp. štruktúru siete, na ktorú útočí. Táto vlastnosť rozhoduje napríklad o tom, či ide o útočníka zo skupiny „insider“ alebo nie a je možné ju určiť napríklad z počtu pokusu o pripojenie.

Motivácia útočníka- rôzne motivácie útočníka sú popísané v podkapitole 10.1.2.

5.1.1 Znalosti útočníka

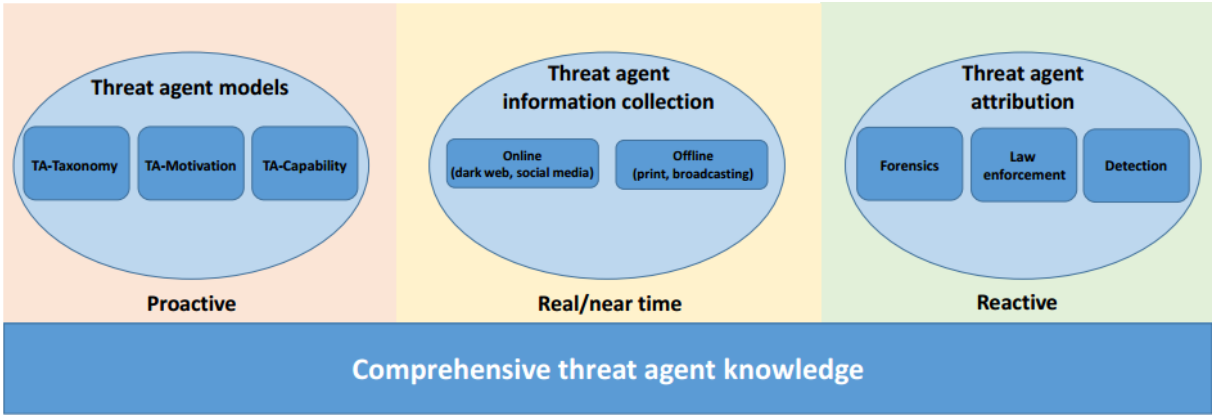
Celková znalosť o útočníkovi pozostáva z troch kategórií znalostí útočníka:

Proaktívne znalosti pokrývajú všetky relevantné parametre ako rôzne skupiny útočníkov, ich schopnosti a zručnosti, ich motivácia, interakcie v skupinách atď. Tieto znalosti sa berú do úvahy pri vyhodnocovaní hrozieb a rizík.

Znalosti v reálnom čase pozostávajú z informácií zozbieraných z online zdrojov ako web či sociálne médiá, z tlače a masmédií. Príkladom týchto znalostí sú inštitúcie, ktorých ukradnuté karty sú ponúkané online. Tento typ znalostí je užitočný pre bezpečnostné operácie a plánovanie, ako aj pre vyhodnocovanie hrozieb a rizík.

Reaktívne znalosti sú výsledkom analýzy rôznych bezpečnostných incidentov. Pomáhajú lepšie chápať činnosť skupín útočníkov, ich motivácie, metódy využívané pri útokoch. Sú poskytované obchodníkmi, právnym vynútením a bezpečnostnými agentúrami po analýze bezpečnostných incidentov. Informácie o insideroch a ich motiváciách viedli k detailným poznatkom tejto skupiny. [12]

Pokrok v tejto oblasti by bol ďalším krokom k zdokonaľovaniu ochrany pred kyberútokmi.



5.1.2 Motivácia útočníka

S každodennými operáciami v takmer každej oblasti spoločnosti, ktoré čím viac závisia od poprepájaných počítačov, stability globálnej ekonomiky či rôznych sociálnych a politických systémov, sa zvyšujú aj požiadavky na spoľahlivé fungovanie internetu a intranetových systémov. Kvôli tomu rastie aj dôležitosť kyberbezpečnosti. Napriek tomu, že vláda a rôzne korporácie sa zameriavajú aj na kybernetickú bezpečnosť, tak globálne zostáva kybernetický priestor zraniteľný a narastá počet zneužitia internetu pre nelegálne činy.

Jednou zo stratégií ako dosiahnuť ciele v oblasti kybernetickej bezpečnosti je zdokonaliť metódy pre klasifikáciu kyberútočníkov. Užitočný prístup ku

klasifikácii útočníkov je vytvorenie typológie, ktorá umožňuje bezpečnostným analytikom účinnejšie identifikovať hrozby založené na známych typoch útočníkov. Takéto typológie umožňujú lepšie pochopiť postupy útočníkov, ale sú náročné na vytvorenie, najmä ak ide o útočníkov, ktorých identity sú často anonymné. Výzvou je preto určiť, kto je páchateľom, aké schopnosti tento páchateľ má a čo ho viedlo k vykonaniu daného činu.

Nikitina [13] opisuje útočenie na počítačové systémy ako spoločenský fenomén- produkt mladých ľudí vyrastajúcich v rozvíjajúcej sa digitálnej dobe s cieľom niečo napadnúť, narušiť, zničiť. Takáto činnosť je považovaná za logicky a sociálne motivovanú kybernetickú aktivitu ako je **hacktivismus** a **crowdsourcing.**

5.1.2.1 Typológie útočníkov

Cieľom každého administrátora kritickej infraštruktúry by malo byť znížiť riziko cenovo čo najefektívnejšie namiesto úplného vylúčenia rizika [14]. Kategorizácia hrozieb je jednou zo stratégií manažmentu rizík. Buyens et al. [15] tvrdia, že jednou z najefektívnejších stratégií manažmentu rizík je vytvoriť **profily útočníkov**, ktoré zahŕňajú najmä úroveň ich schopností.

Kategorizácia má niekoľko výhod: [16]

umožňuje systematické štúdium bezpečnostných incidentov,

pomáha manažérom budovať efektívne obranné systémy, ktoré sú menej zraniteľné,

uľahčuje nahlasovanie incidentov kompetentným tímom.

Landreth [17] navrhol 5 typov útočníkov založených na ich schopnostiach a motiváciách. Medzi možné motivácie útočníka zaraďuje zámerné spôsobenie škody, intelektuálnu výzvu, vzrušenie, zvýšenie ega a kriminálny zisk. Chantler [18] kategorizuje útočníkov podľa motivácií, schopností a skúseností.

Ideálne by bolo rozlišovať útočníkov na základe viacerých parametrov ako identita páchateľov a ich cieľ, metóda útoku a frekvencia výskytu, cieľ, ktorý chce útočník dosiahnuť a spôsobená škoda. Avšak keďže takéto údaje sú k dispozícii len zriedka, tak reálnejšie je klasifikovať útočníkov len podľa schopností a motivácií (pomsta, finančný zisk, zvedavosť, notoričnosť). V niektorých modeloch sa môžeme stretnúť aj s ideológiou ako jednou z foriem motivácie útočníka. Medzi ideologické motivácie môžeme zaradiť nacionalizmus alebo náboženstvo. Ako heckeri sú väčšinou

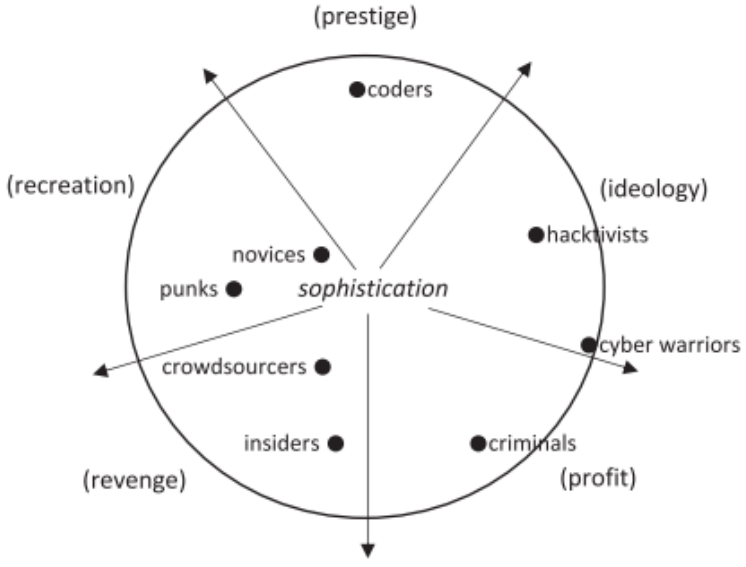
označovaní politickí aktivisti. Rogers's [19] však upravil taxonómiu tak, že o hacktivistoch hovorí ako o útočníkoch, ktorí chcú predovšetkým získať notoričnosť a politické motivácie sú pre nich až druhoradé.

S rozvojom internetu sa postupne menilo aj zloženie jeho používateľov a s rôznorodými typmi používateľov sa začali objavovať aj rôznorodé škodlivé aktivity vďaka rozvíjajúcim sa schopnostiam útočníkov a ich motiváciám. Okrem hacktivistov sa v poslednom čase objavil aj ďalší typ útočníckej skupiny, **crowdsourcing.** Online crowdsourcing pozostáva z kolektívnej snahy vyriešiť nejaký problém väčšinou s využitím nelegálnej činnosti a dosiahnuť tým pochybné ciele. Tento typ činnosti zahŕňa takzvaný **doxing**, čo je využívanie internetových zdrojov (napríklad aj nabúranie sa do účtov na rôznych sociálnych sieťach) na získavanie osobných údajov o konkrétnych používateľoch.

Glenny [20] vo svojej práci zhrnul, že chápanie schopností a motivácií kybernetických útočníkov prispieva vo veľkej miere k vývoju bezpečnosti rôznych systémov, ktoré sú závislé na technických riešeniach.

5.1.2.2 Circumplex model

Kruhové modely sú používané na prezentovanie rôznych konceptov a vzťahov medzi nimi. Seebruck [21] vo svojom článku modifikoval tento model tak, že kruh je rozdelený do štyroch kvadrantov, kde každý z nich reprezentuje nejakú motiváciu. Dôležité je umiestnenie jednotlivých skupín útočníkov. Skupiny blízko vedľa seba sú si podobné, umiestnenie skupiny blízko okraja kvadrantu indikuje, že motivácie sa prekrývajú a pozície ďalej od centra naznačujú pokročilejšie schopnosti útočníka.

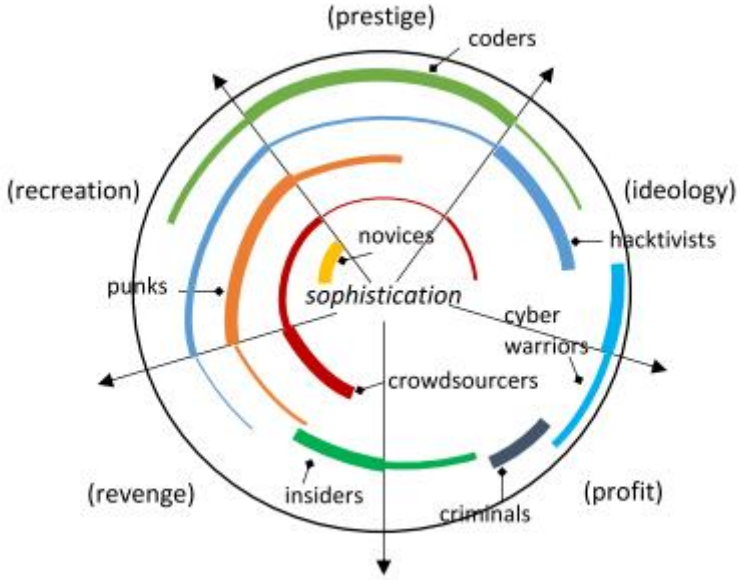


Takýto model je užitočný na zobrazenie vzťahov medzi útočníkovými schopnosťami a motiváciami, čo pomáha pri identifikácii a kategorizácii útočníkov. Seebruck teda navrhol tieto typy útočníkov a zoradil ich podľa narastajúcich technických zručností: **nováčikovia, crowdsourceri, pankáči, hacktivisti, insideri, kriminálnici a kybernetickí bojovníci.** Na obrázku vidíme, že každá z piatich motivácií- ideológia, profit, pomsta, zábava, prestíž- má vlastnú oblasť.

Na obrázku pozícia hacktivistov vyjadruje ich stredne pokročilé schopnosti, to, že ich motiváciou je určitá ideológia. Pozícia kybernetických bojovníkov indikuje vysoko sofistikovaných útočníkov motivovaných ideológiou a ziskom. Kriminálnici majú schopnosti na vyššej úrovni a primárne sú motivovaní ziskom, sekundárne pomstou.

5.1.2.3 Vážený circumplex model

I keď sú circumplex modely užitočné na zobrazovanie vzťahov medzi rôznymi typmi útočníkov, ich schopnosťami a motiváciami, neberú do úvahy napríklad to, ak má útočník nie jednu, ale niekoľko motivácií súčasne. Kvôli tomu bol navrhnutý vážený circumplex model, ktorý umožňuje zobraziť niekoľko motivácií útočníka naraz. Namiesto bodov v jednotlivých sektoroch sa využívajú krivky, ktoré môžu prechádzať cez viacero sektorov. To, ako veľmi bol útočník ovplyvnený daným typom motivácie znázorňuje hrúbka krivky.



5.1.2.4 Využitie circumplex modelu

Tieto modely môžu byť využívané na odhaľovanie vzťahov, ako napríklad čierne trhy v oblasti profitu dosiahnuteľné cez Tor. Môžu byť použité na zobrazenie nepriamych vzťahov a na odhaľovanie komplexných vzťahov medzi hackermi a počítačovými systémami. Sú veľmi užitočným investigatívnym nástrojom vďaka ich rýchlej vizualizácii hrozieb.

6 Analýza údajov

Pre účely diplomovej práce máme k dispozícii týždenné údaje zachytené honeypotom, ktoré nám poskytol CESNET. Ide približne o 16 miliónov záznamov, pričom každý riadok je vo formáte IDEA, teda prakticky ide o JSON formát. IDEA je deskriptívny dátový model, pre ktorý je typický *key:value* formát. Okrem toho má definovanú maximálnu hĺbku vnorenia 2.

Aby sa nám s údajmi lepšie pracovalo, sú uložené v postgreSQL databáze v tabuľke, ktorá pozostáva z dvoch stĺpcov: ID a ideadata. Záznamy v stĺpci ideadata sú priamo v IDEA formáte, ale vďaka postgreSQL vieme efektívne pracovať aj s JSON objektami.

Pomocou nasledovných dopytov sme z údajov, ktoré máme k dispozícii získali všetky kľúče, ktoré sa v našich údajoch vyskytujú na prvej úrovni IDEA formátu a na druhej úrovni pre kľúč „Source“, teda získali sme informácie o zdroji útoku:

```
select distinct jsonb_object_keys(ideadata) from ideas;

select distinct jsonb_object_keys(ideadata->'Source'->0) from ideas;
```

Z výsledkov týchto dopytov, teda z dostupných údajov o útoku vo formáte IDEA budeme uvažovať nasledovné:

- Category
- Duration, resp. rozdiel medzi CeaseTime a DetectTime
- Source
    - IP4
    - Proto
    - Port

Na to, aby sme určili skupiny útočníkov, budeme využívať zhlukovací algoritmus nad týmito údajmi. Najskôr ich však potrebujeme predspracovať a vytvoriť z nich súbor vo formáte .arff, ktorý bude vstupom pre zhlukovací algoritmus k-means v nástroji Weka.

7 Návrh riešenia

7.1.1 Predspracovanie údajov

Pre každú IP adresu (Source.IP4) bude vo vstupnom súbore jeden záznam-riadok, ktorý bude mať nasledovnú štruktúru:

IP, Category(konkrétny počet výskytu pre danú kategóriu), Duration, Proto(konkrétny počet výskytu pre daný protokol), Port (konkrétne počty výskytu pre daný port).

V údajoch sa nachádzajú nasledovné typy útokov:

Recon.Scanning, Attempt.Login, Attempt.Exploit, Intrusion.Botnet, Anomaly.Traffic, (Malware, Test), (Other, Test), Abusive.Spam, (Fraud.Phishing, Test), Availability.DoS, Anomaly.Connection, (Recon.Scanning, Anomaly.Protocol, Test), Vulnerable.Config, Availability.DDoS, (Attempt.Login, Test), (Attempt.Exploit, Test), (Recon.Scanning, Test), (Itrusion.Botnet, Test), (Itrusion.Botnet, Malware), (Abusive.Spam, Test), (Attempt.Exploit, Malware), (Availability.DoS, Test)

kategoria	pocet
["Recon.Scanning"]	15924769
["Other", "Test"]	160210
["Attempt.Login", "Test"]	128568
["Recon.Scanning", "Test"]	89947
["Attempt.Exploit", "Test"]	73984
["Intrusion.Botnet", "Test"]	59037
["Attempt.Login"]	23554
["Anomaly.Traffic"]	12601
["Attempt.Exploit"]	10580
["Intrusion.Botnet", "Malware"]	6833
["Abusive.Spam"]	4674
["Abusive.Spam", "Test"]	4208
["Fraud.Phishing", "Test"]	3483
["Availability.DoS"]	3427
["Malware", "Test"]	3404
["Attempt.Exploit", "Malware"]	630
["Availability.DoS", "Test"]	224
["Anomaly.Connection"]	39
["Recon.Scanning", "Anomaly.Protocol", "Test"]	12
["Intrusion.Botnet"]	6
["Vulnerable.Config"]	1
["Availability.DDoS"]	1

Protokoly vyskytujúce sa v údajoch:

TCP, SSH, SMTP, (tcp, telnet), FTP, http, UDP, IMAP, (udp, dns), SIP, (tcp, ssh), (tcp, ms-wbt-server)

proto	pocet
["tcp"]	1166828
["tcp", "ssh"]	66538
["smtp"]	53676
["tcp", "ms-wbt-server"]	40753
["tcp", "telnet"]	18207
["ssh"]	11238
["ftp"]	3512
["http"]	2948
["udp"]	2668
["imap"]	2464
["udp", "dns"]	609
["sip"]	146
["TCP"]	67
["UDP"]	13
NULL	0

Náš prvý krok bol získanie potrebných, vyššie popísaných údajov z PostgreSQL tabuľky. Využili sme nasledovný dopyt:

select * from (select ideadata->'Source'->0->'IP4' as IP, ideadata->'Category' as category, count(ideadata->'Category') as countCategory, ideadata->'Source'->0->'Proto' as protocol, count(ideadata->'Source'->0->'Proto') as countProto from ideas where id<3000000 group by ideadata->'Category', ideadata->'Source'->0->'Proto', ideadata->'Source'->0->'IP4' order by ideadata->'Source'->0->'IP4') as t where t.protocol is not null

Výsledkom boli údaje v nasledujúcom tvare:

ip	category	countcategory	protocol	countproto
["10.106.235.3"]	["Recon.Scanning"]	1	["tcp"]	1
["10.10.93.2"]	["Recon.Scanning"]	5	["tcp"]	5
["101.108.78.173"]	["Recon.Scanning"]	1	["tcp"]	1
["101.68.209.91"]	["Recon.Scanning"]	2	["tcp"]	2
["103.23.137.25"]	["Recon.Scanning"]	4	["tcp"]	4
["103.23.139.152"]	["Recon.Scanning"]	2	["tcp"]	2
["103.29.124.103"]	["Attempt.Login", "Test"]	1	["tcp", "telnet"]	1
["103.37.164.23"]	["Recon.Scanning"]	4	["tcp"]	4
["103.37.165.250"]	["Recon.Scanning"]	4	["tcp"]	4
["103.37.167.239"]	["Recon.Scanning"]	5	["tcp"]	5
["103.5.126.158"]	["Recon.Scanning"]	3	["tcp"]	3
["103.55.90.30"]	["Recon.Scanning"]	1	["tcp"]	1
["104.175.13.83"]	["Attempt.Login", "Test"]	1	["tcp", "telnet"]	1
["104.207.141.110"]	["Recon.Scanning"]	5	["tcp"]	5
["106.184.1.178"]	["Recon.Scanning"]	5	["tcp"]	5
["106.184.4.52"]	["Recon.Scanning"]	4	["tcp"]	4
["106.185.43.131"]	["Recon.Scanning"]	5	["tcp"]	5
["106.186.113.169"]	["Recon.Scanning"]	5	["tcp"]	5
["106.186.20.183"]	["Recon.Scanning"]	3	["tcp"]	3
["106.187.45.144"]	["Recon.Scanning"]	5	["tcp"]	5
["106.187.52.160"]	["Recon.Scanning"]	2	["tcp"]	2
["106.187.97.102"]	["Recon.Scanning"]	5	["tcp"]	5
["106.75.31.144"]	["Recon.Scanning"]	1	["tcp"]	1
["107.151.189.44"]	["Recon.Scanning"]	1	["tcp"]	1
["10.8.13.14"]	["Recon.Scanning"]	1	["tcp"]	1
["109.190.229.147"]	["Recon.Scanning"]	2	["tcp"]	2
["109.226.27.212"]	["Recon.Scanning"]	5	["tcp"]	5
["109.95.207.29"]	["Recon.Scanning"]	2	["tcp"]	2
["110.78.151.37"]	["Attempt.Login", "Test"]	3	["tcp", "telnet"]	3
["110.87.16.126"]	["Recon.Scanning"]	3	["tcp"]	3

Aby sme tieto údaje pretransformovali do požadovaného formátu, napísali sme metódu v jave, ktorá vytvorila súbor so záznamami typu

101.201.77.248,0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 373, 0, 0, 0, 0, 0, 0, 0,0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 373, 0.

Takýto riadok teda hovorí, že z IP adresy 101.201.77.248 bol 373-krát zaznamenaný útok typu (Attempt.Login, Test) a bol použitý protokol TCP a SSH. Aby bol tento súbor vhodný ako vstup pre klastrovanie v nástroji Weka, upravili sme ho do .arff formátu tým, že sme pridali informácie o názvoch a typoch jednotlivých atribútov.

7.1.2 Porovnanie zhlukovacích algoritmov

Rozoznávanie vzorov v údajoch je založené na priradení objektu do jednej z kategórií na základe jeho vlastností, čo zdôrazňuje jeho príslušnosť do určitej skupiny. Zhlukovanie je jeden zo spôsobov učenia bez dozoru. Cieľom je získanie skupín objektov, ktoré sú si navzájom podobné.

K-means klastrovanie

K-means algoritmus je jeden z najjednoduchších zhlukovacích algoritmov, ktorý sa používa na získanie zadefinovaného počtu skupín objektov založených na ich atribútoch. Ide o numerickú, nedeterministickú a iteratívnu metódu na klasifikáciu dát.

Výhody: časová zložitosť

Jednoduchosť

Nevýhody: Je potrebné hneď na začiatku určiť počet zhlukov

Zložitá identifikácia počiatočných zhlukov

Výsledné zhluky závisia od počiatočných zhlukov

Aglomeratívne klastrovanie

Ide o deterministický algoritmus, ktorý na výstup dáva hierarchickú štruktúru, ktorá nepotrebuje mať vopred špecifikovaný počet klastrov. Každý klaster má svoje podklastre a tie majú svoje podklastre atď.

Výhody: Výsledkom sú pomerne malé zhluky, ktoré sú jednoduchšie na analýzu

Počet zhlukov nie je potrebné definovať hneď na začiatku

Nevýhody: Výsledok závisí od použitej metriky pre určovanie vzdialenosti

Ak sú objekty zoskupené nesprávne v počiatočnej fáze, tak v neskorších fázach už nemôžu byť preusporiadané

Rozdeľovacie klastrovanie

Tento druh klastrovacích algoritmov funguje podobne ako aglomeratívne klastrovanie s tým rozdielom, že prebieha v opačnom smere- zhora nadol. Algoritmus začína s jedným zhlukom ktorý obsahuje všetky objekty a postupne ho rozdeľuje až pokiaľ nezostanú zhluky obsahujúce jednotlivé objekty.

Výhody: Hneď na začiatku sú k dispozícii všetky údaje a preto sa dosahujú najlepšie výsledky

Nevýhody: Časová zložitosť

Výsledky závisia od použitej metriky pre určovanie vzdialenosti. [1]

Na určenie zhlukov, teda skupín útočníkov, používame nástroj Weka. V tomto nástroji je k dispozícii niekoľko klastrovacích algoritmov. Na základe predošlej analýzy sme sa rozhodli použiť pre účely našej diplomovej práce algoritmus K-means.

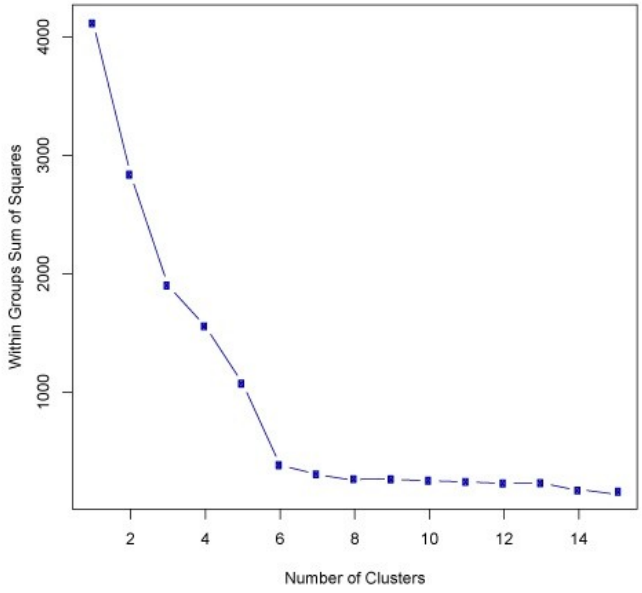
7.1.3 Určenie vhodného „k“ pre k-means zhlukovanie

Na určenie vhodnej konštanty „k“ pre k-means zhlukovanie na predspracovaných údajoch sme využili tzv. „elbow“ metódu. Jej hlavná myšlienka spočíva v spustení k-means algoritmu určitý počet krát a pre každé „k“ vypočítať tzv. „sum of squared errors“ (SSE) podľa vzorca

$$SSE = \sum_{i=1}^{K} \sum_{x \in c_i} dist(x, c_i)^2$$

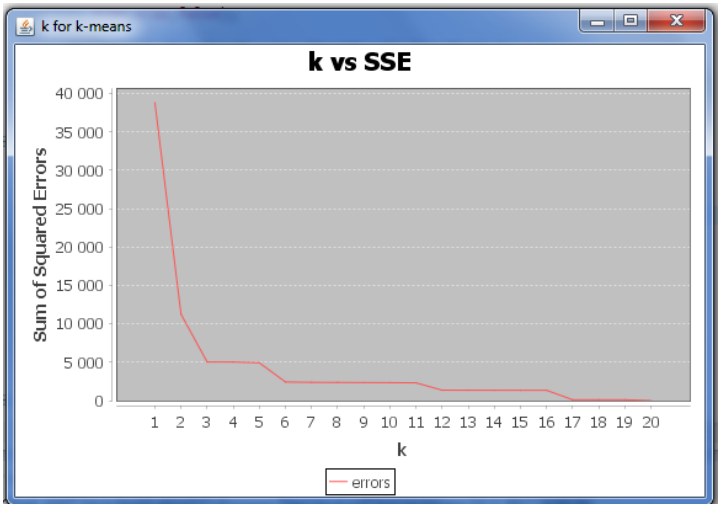
.

SSE je teda definované ako súčet vzdialeností umocnených na druhú medzi každým prvkom klastra a stredom príslušného klastra. Zväčšovaním „k“ sa SSE zmenšuje ako je vidno na nasledujúcom obrázku:



Dôvodom je to, že s narastajúcim počtom klastrov sa tieto klastre zmenšujú a teda aj skreslenie sa zmenšuje. Cieľom „elbow“ metódy je zvoliť také „k“, pre ktoré hodnota SSE náhle poklesne. Pre prípad na obrázku by táto metóda ako „k“ zvolila 6, pretože pre k=7 a vyššie je zmena v SSE už len nepatrná.

Na implementáciu tejto metódy sme využili knižnicu Weka v našom JAVA kóde, ktorá okrem iného umožňuje vykonávať k-means algoritmus a pre každé „k“ navyše počíta aj SSE. Nechali sme spočítať SSE pre „k“ od 1 do 20 a výsledky sme uložili do poľa *errors*. Tieto zapamätané hodnoty sme následne zobrazili v čiarovom grafe pomocou knižnice JFreeChart. Pre naše predspracované údaje bol výsledok nasledovný:



Teda pre naše údaje sme zvolili k=6.

7.1.4 Klastrovanie a analýza výsledkov

Na predspracovaných údajoch sme v nástroji Weka spustili k-means algoritmus pričom ako parameter „k“ sme zvolili 6. Výsledok klastrovania sme uložili do súboru, teda tento súbor obsahuje jednotlivé inštancie a ku každej inštancii aj informáciu o tom, do akej skupiny patrí (hodnoty „cluster0“ až „cluster5“).

Následne sme pomocou metódy v JAVE pre každý klaster, teda pre každú skupinu útočníkov, určili, aké typy útokov táto skupina vykonáva a aké protokoly využíva. Pomenujme získané skupiny útočníkov A0, A1, A2, A3, A4, A5. O týchto skupinách máme teda nasledovné informácie:

A0

- Útoky: Anomaly.Traffic, (Itrusion.Botnet, Test)
- Protokoly: UDP, TCP

A1

- Útoky: (Attempt.Exploit, Test)
- Protokoly: FTP, SIP, http, IMAP

A2

- Útoky: (Attempt.Exploit, Test)
- Protokoly: SMTP

A3

- Útoky: Recon.Scanning
- Protokoly: TCP

A4

- Útoky: Anomaly.Traffic, Vulnerable.Config, (Recon.Scanning, Test), Recon.Scanning, Availability.DoS, (Attempt.Login, Test)
- Protokoly: UDP, (udp, dns), (tcp, ms-wbt-server), (tcp, ssh), (tcp, telnet), TCP

A5

- Útoky: (Attempt.Exploit, Test)
- Protokoly: SSH

7.1.5 Zaradenie nového útočníka do skupiny

Na to, aby sme vedeli zaradiť nový záznam do príslušnej skupiny útočníkov, predpokladáme, že už máme vopred naučený systém tak, ako bolo popísané v predchádzajúcich podkapitolách.

Nový záznam je celočíselný vektor a teda vieme určiť jeho vzdialenosť od každého vektora nachádzajúceho sa v už zaradenej množine vektorov teda útočníkov. Využijeme vzorec:

$$\sqrt{\sum_{i=1}^{n}(q_i - p_i)^2}.$$

Tento nový záznam zaradíme do tej skupiny, v ktorej sa nachádza aj záznam, ku ktorému má najbližšie.

8 Zoznam použitej literatúry

[1] Towards Modelling Adaptive Attacker's Behaviour, Leanid Krautsevich, Fabio Martinelli, and Artsiom Yautsiukhin

[2] Attacker Classification to Aid Targeting Critical Systems for Threat Modelling and Security Review, Rocky Heckman

[3] Adversary Characterization and Scoring Systems by Marcus H. Sachs, P.E., Researcher / Instructor, The SANS Institute.Tom Parker, Head Of Research, Pentest Ltd (UK).Eric D. Shaw, Ph.D., Clinical Psychologist, Consulting & Clinical Psychology. Ltd. And Toby Miller, Researcher

[4] Attacker Profiling in Quantitative Security Assessment Based on Attack Trees Aleksandr Lenin, Jan Willemson, and Dyan Permata Sari

[5] Towards Practical Attacker Classification for Risk Analysis in Anonymous Communication, Andriy Panchenko and Lexi Pimenidis

[6] A framework for the motivation of attackers in attack tree analysis, Rick van Holsteijn, Wolter Pieters, Maarten Franssen, Jan van den Berg, Pieter van Gelder

[7] A. Hirt, M. J. Jacobson, and C. Williamson. Survey and analysis of anonymous communication schemes. Submitted to ACM Computing Surveys, Department of Computer Science, University of Calgary, December 2003.

[8] J.-F. Raymond. Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems. In H. Federrath, editor, Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability, pages 10–29. Springer-Verlag, LNCS 2009, July 2000

[9] JOSHI, R.C. – SARDANA A. 2011. Honeypots: A New Paradigm to Information Security. Science Publishers, 2011.

[10] Tomasz Grudziecki et al. Proactive Detection of Security Incidents Honeypots 2012-11-20

[11] Symantec Corporation, White paper: Web based attacks

[12] Louis Marinos, Adrian Belmonte, Evangelos Rekleitis, ENISA Threat Landscape 2015

[13] Nikitina Svetlana. Hackers as tricksters of the digital age: creativity in hacker culture. J Pop Cult 2012;45(1):133e52.

[14] Friedman Jon, Hoffman Daniel v. Protecting data on mobile devices: a taxonomy of security threats to mobile computing and review of applicable defenses. Inf Knowl Syst Manag 2008;7:159e80.

[15] Buyens Koen, De Win Bart, Joosen Wouter. “Empirical and statistical analysis of risk analysis- driven techniques for threat management.” IEEE computer society, the first international workshop on secure software engineering. Vienna: Austria; 2007. April 10e13. (accessed 09.04.15), https://lirias.kuleuven.be/bitstream/123456789/146252/1/ paper.pdf

[16] Farahmand Fariborz, Sharp Gunter P, Enslow Philip H. A management perspective on risk of security threats to information systems. Inf Technol Manag 2005;6:203e25.

[17] Landreth Bill. Out of the inner circle: a hacker's guide to computer security. Microsoft Press; 1985.

[18] Chantler Nicholas. Profile of a computer hacker. florida: infowar; 1996

[19] Rogers Marcus K. The psyche of cybercriminals: a psycho-social perspective. In: Ghosh Sumit, Turrini Elliot, editors. Cybercrimes: a multidisciplinary analysis. Springer; 2010. p. 217e35

[20] Glenny Misha. Dark market: how hackers became the new mafia. New York: Vintage; 2011

[21] Seebruck, Ryan. "A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model." Digital Investigation 14 (2015): 36-45.