Technická univerzita v Košiciach
Fakulta elektrotechniky a informatiky

Rozšírenie nástroja SLAmeter o detekciu anomálií v počítačových sieťach

Diplomová práca

Príloha A

POUŽÍVATEĽSKÁ PRÍRUČKA bmIDS v2.3

Študijný program:	Informatika
Študijný odbor:	9.2.1 Informatika
Školiace pracovisko:	Ústav výpočtovej techniky (ÚVT)
Vedúci práce:	Ing. Adrián Pekár, PhD.
Konzultant:	Ing. Ján Juhár

Košice 2015 **Bc. Ladislav Berta**

Obsah

Zoznam obrázkov

Zoznam tabuliek

1 Funkcia programu

Systém bmIDS predstavuje nástroj pre detekciu narušenia v počítačových sieťach. Pozostáva z dvoch aplikácií, analyzéra *bmIDSanalyzer* a aplikácie *ids*, ktorá je súčasťou webovej aplikácie SLAmeter. Analyzér *bmIDSanalyzer* je konzolová aplikácia, ktorého úlohou je vyhodnotenie a spracovanie údajov o prebiehajúcej komunikácii v sieti, a na základe výsledkov vyhodnotenia a fuzzy logiky určiť mieru pravdepodobnosti útokov. Zdrojom údajov pre systém bmIDS sú nástroje exportér (mybeem) a kolektor (JXColl), ktoré zabezpečujú monitorovanie siete a poskytujú informácie analyzéru v podobe správ IPFIX protokolu. Prenos správ je zabezpečený aplikačným rozhraním ACP, ktoré správy od kolektora poskytuje v reálnom čase. Kolektor okrem poskytovania údajov o sieti slúži aj na ukladanie údajov do databázy, ktorá analyzéru slúži v režime učenia, kedy vytvára obraz štandardnej prevádzky. V režime detekcie je analyzér spustený na serveri kde neustále vyhodnocuje sieťovú prevádzku. V prípade zaznamenania útokov zapisuje údaje o kritickej prevádzke do databázy, a zároveň môže odosielať vyhodnotené údaje aj webovej aplikácii ids ako aj emailové notifikácie pre používateľa s detailami o útoku. Webová aplikácia ids pozostáva z dvoch sekcií, zo sekcie *Monitorovania* a sekcia *Záznamy útokov*. Sekcia *Monitorovania* umožňuje používateľovi sledovať vyhodnotenú prevádzku v reálnom čase, pričom sekcia *Záznamy útokov* slúži pre zobrazovanie historických záznamov získaných z databázy.

2 Inštalácia programu

2.1 Požiadavky na technické prostriedky

Pre zaistenie spoľahlivého behu bmIDS analyzéra sa vyžaduje nasledovná hardvérová konfigurácia:

- CPU Intel Pentium III 1GHz alebo ekvivalent
- RAM 1 GB
- HDD 100 MB voľného priestoru
- sieťová karta 100Mbit/s

Webová aplikácia ids sa neinštaluje, ale je dostupná vo webovej aplikácii nástroja SLAmeter. Požiadavky na technické prostriedky a samotná inštalácia webovej aplikácie tohto nástroja sú uvedené v príslušnej dokumentácii. Inštalácia exportéra a kolektora sa prevedie tiež podľa príslušnej dokumentácie.

2.2 Požiadavky na programové prostriedky

Spustenie bmIDS analyzéra vyžaduje:

- operačný systém Linux alebo Windows, ale odporúča sa Linux/Ubuntu
- Java Runtime Enviroment (JRE 6.0)
- databázový server PostgreSQL 7.3 a vyšší
- aplikáciu kolektora JXColl v3.9 podľa jej dokumentácie
- aplikáciu exportéra mybeem podľa jej dokumentácie

2.3 Vlastná inštalácia

Pred inštaláciou samotného bmIDS je potrebné pridať tabuľky pre ukladanie údajov o útokoch do databázy. Je to možné dvoma spôsobmi:

- pred prvým spustením analyzéra nasadiť webovú aplikáciu nástroja SLAmeter, pri ktorej inštalácii sa použije príkaz *python manage.py syncdb* a vytvoria sa príslušné tabuľky
- vytvorenie tabuliek zo skriptu, ktorý obsahuje stiahnutá adresárová štruktúra (tento spôsob sa má použiť v prípade ak aplikácia bmIDSanalyzer sa nepoužíva s webovou aplikáciou)

2.3.1 BmIDSanalyzer

Aplikácia bmIDSanalyzer má byť inštalovaná na serveri kde je nasadená webová aplikácia nástroja SLAmeter. V prípade nepoužitia webovej aplikácia môže byť nástroj bmIDSanalyzer inštalovaný na ľubovoľný server.

Pre úspešnú inštaláciu v operačnom systéme Ubuntu (Linux) je potrebné vykonať:

1. Stiahnuť inštalačný súbor z GIT
   `wget https://git.cnl.tuke.sk/monica/slameter_ids/blob/master/bmIDSanalyzer/bin/bmIDS.tar.gz --no-check-certificate`
2. Rozbaliť ho
   `tar -xzvf bmIDS.tar.gz`
   výsledkom bude adresárová štruktúra, ktorá bude obsahovať spustiteľný .jar súbor a potrebné konfiguračné súbory
3. Následne je možné konzolovú aplikáciu spustiť príkazom
   `java -jar bmIDSanalyzer.jar` pričom voliteľnými parametrami sú:
   - *konfiguračný súbor* - ak sa nezadá, použije sa predvolený `config.xml`

- *parameter -l* – spustí režim učenia a aplikácia si bude pýtať dátum, ktorý má zodpovedať dátumu záznamov v databáze z ktorého sa naučia štandardné hodnoty prevádzky

2.3.2 Wbová aplikácia *ids*

Pre dostupnosť webovej aplikácie *ids* nie je potrebná inštalácia, ale je potrebné nasadenie webovej aplikácie SLAmeter podľa príslušnej dokumentácie. Po úspešnom nasadení bude aplikácia *ids* dostupná vo webovej aplikácii nástroja SLAmeter, ktorá by mala byť prístupná na adrese inštalovaného servera.

3 Použitie programu

Konzolovú aplikáciu bmIDSanalyzer môžeme spustiť príkazom:

```
java --jar bmIDSanalyzer.jar
```

voliteľné parametre sú:

- konfiguračný súbor (predvolené config.xml)
- parameter –l (spustí režim učenia)

Pred spustením detekcie je potrebné ešte spustiť zhromažďovací proces (JXColl) a exportovací proces (mybeem). Zároveň je potrebné spustiť databázový server s odpovedajúcou databázou (*bmdb*) v ktorej sa nachádzajú historické záznamy potrebné pre režim učenia a tiež je potrebný prístup k databáze (*slaweb*) do ktorej sa ukladajú údaje o podozrivej prevádzke.

Webovú aplikáciu ids spustíme tak, že do adresného riadku internetového prehliadača zadáme adresu:

```
http://[IP adresa servera]:9000/app/ids
```

Sledovanie vyhodnocovanej prevádzky v sekcii *Monitorovanie* je možné iba v tom prípade ak je spustený bmIDSanalyzer a samozrejme komponenty exportér a kolektor.

3.1 Popis dialógu s používateľom

3.1.1 bmIDSanalyzer

Konzolová aplikácia bmIDSanalyzer, neposkytuje grafické rozhranie pre komunikáciu s používateľom. Po spustení príkazu *java –jar bmIDSanalyer.jar* sú v konzole zobrazované informácie o spustení, o načítanom konfiguračnom súbore a chybové

hlásenia. Ak pri spustení bol zvolený režim učenia, používateľ má možnosť zvoliť deň učenia, po ktorom sa aplikácia pripojí na databázový server a naučením získa štandardné hodnoty následne ktoré je možné uložiť do konfiguračného súboru. Výpis informačných hlásení po úspešnom spustení aplikácie v režime učenia je zobrazené na obrázku Obr. 3 – 2. Spustenie programu v režime detekcie zobrazuje obrázok Obr. 3 – 1. Program je možné ukončiť klávesovou kombináciou Ctrl + c.

```
lacke@lacke-M51Vr:~/000_analyzer_bmIDS$ java -jar bmIDSanalyzer.jar -l
Starting bmIDS v2.3
No configuration file was given.
Loading data from configuration file from it's default location: config.xml
Data from configuration file have been successfully loaded.
Starting LEARN MODE.
Type learning date (dd.mm.yy):
13.04.2015
=========================
  Database information
=========================
IP address: 127.0.0.1
Port:       5432
Name:       bmdb
Login:      bm
Password:   bm
=========================
Number of records in database = 101765
Learning.....
.
.
Learning finished.
----------------------
Learning results:

psMaxFlowCount=   9
sfMaxSynCount=    14
ufMaxPacketCount= 120
rfMaxRstCount=    18
tfMaxTtlCount=    0
ffMaxFinCount=    12

Save? [y/n]
y
Learned values have been saved in file.
Finished learning.
Should continue with detection?[y]
```

Obr. 3 – 1 Spustenie aplikácie bmIDSanalyzer v režime detekcie

```
lacke@lacke-M51Vr:~/000_analyzer_bmIDS$ java -jar bmIDSanalyzer.jar
Starting bmIDS v2.3
No configuration file was given.
Loading data from configuration file from it's default location: config.xml
Data from configuration file have been successfully loaded.
-------------------------------------
Loaded values from config file:
psMaxFlowCount: 9
sfMaxSynCount: 14
ufMaxPacketCount: 120
rfMaxRstCount: 18
tfMaxTtlCount: 0
ffMaxFinCount: 12
sendMail: true
mailFrom: bmidsanalyzer@gmail.com
mailFromPwd: 123456
mailTo: lacke.g@gmail.com
slawebDbIP: 127.0.0.1
slawebDbPort: 5432
slawebDbName: slaweb
slawebDbLogin: slawebuser
slawebDbPassword: slaweb
-------------------------------------
Starting DETECTION MODE.
```

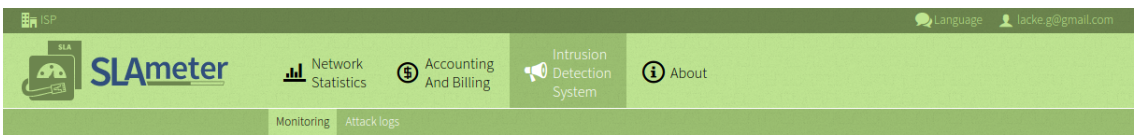
Obr. 3 – 2 Spustenie aplikácie bmIDSanalyzer v režime učenia

3.1.2 Webová aplikáci *ids*

Aplikácia *ids* sa nachádza vo webovej aplikácii SLAmeter pod názvom *Intrusion Detection System*. Pod touto aplikáciou sa nachádzajú dve sekcie:

- **Monitorovanie** – *Monitoring* – umožňuje sledovať vyhodnocovanie prevádzky v sieti
- **Záznamy útokov** – *Attack logs* – umožňuje zobraziť údaje o podozrivej prevádzke z rôzneho časového obdobia a zobrazenie detailov o vybranom útoku

Aplikácia *ids* v rámci webovej aplikácie SLAmeter je zobrazená na obrázku Obr. 3 – 3)

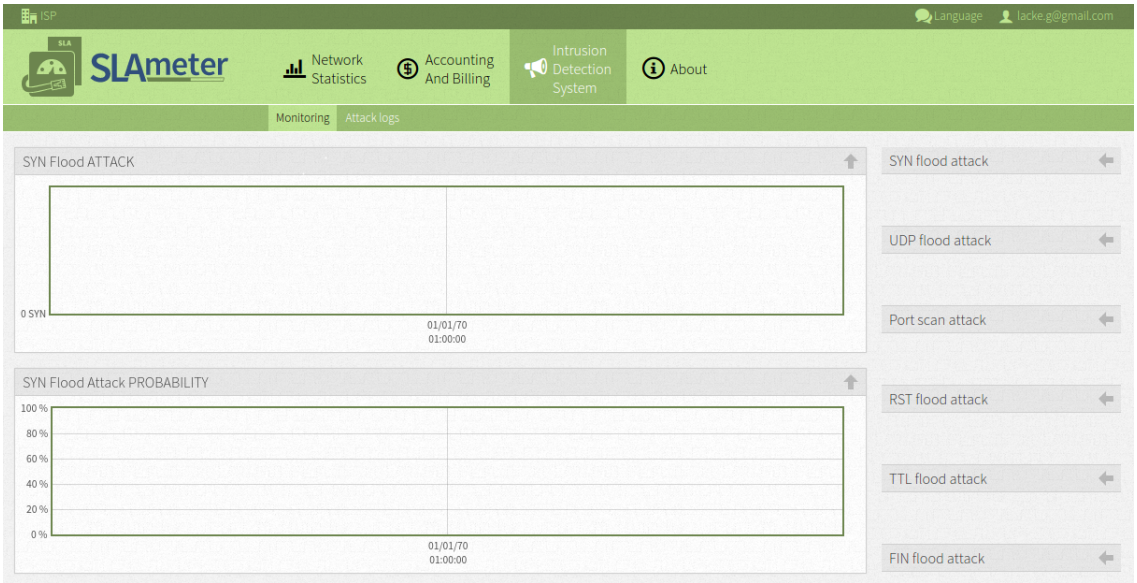


Obr. 3 – 3 Aplikácia *ids* v rámci webovej aplikácie SLAmeter

3.2 Popis funkcií programu

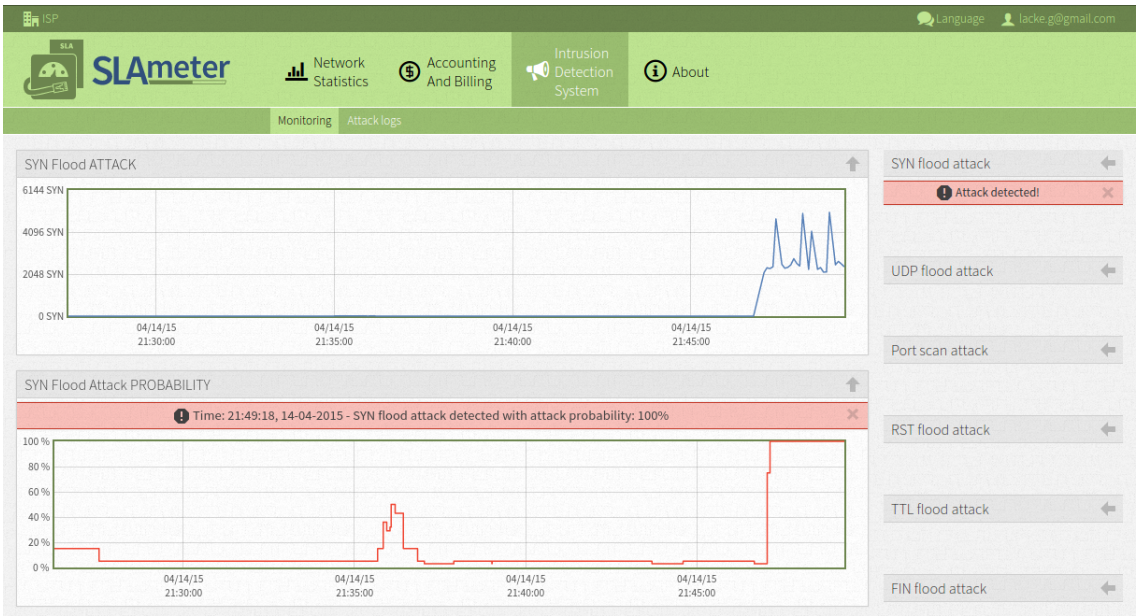
3.2.1 Monitoring reálnej prevádzky

Po kliknutí na aplikáciu ids v rámci webovej aplikácie SLAmeter sa zobrazí sekcia monitorovania. Webová aplikácia pošle požiadavku pre analyzér na prijímanie údajov. Ak je analyzer spustený, začne posielať vyhodnotené údaje a používateľovi sa tieto údaje zobrazia v podobe grafov. Pre každý typ útoku existujú dva grafy. Jeden je určený na zobrazovanie sledovaných charakteristík útoku a druhý, nachádzajúci sa pod ním, zobrazuje pravdepodobnosť prieniku pre daný útok. Pre sledovanie priebehu vyhodnocovania sú hodnoty v grafoch zobrazované v závislosti na čase. Aktualizácia jednotlivých grafov závisí od vyhodnotenia údajov analyzérom, po každom vyhodnotení sa príslušné grafy aktualizujú. Grafické priebehy sa dajú skryť respektíve znova zobraziť. Pre navigáciu po stránke slúži navigačná časť umiestnená v pravej časti sekcie monitorovania. Po kliknutí na šípku pre zvolený typ útoku sa zobrazia príslušné grafové sekcie. Sekcia monitorovania s grafickými priebehmi pre SYN záplavový útok je zobrazená na obrázku Obr. 3 – 4)



Obr. 3 – 4 Sekcia monitorovania – *Monitoring* po otvorení aplikácie *ids*

V prípade zaznamenania útoku sa v príslušnom grafickom module zobrazí výstražná správa s informáciami ako dátum, čas a pravdepodobnosť kedy bol útok zaznamenaný. Táto výstražná správa má za úlohu upútať pozornosť používateľa a preto sa zobrazuje aj v navigačnej časti sekcie. Sekciu monitorovania v prípade zaznamenania SYN záplavového útoku zobrazuje obrázok Obr. 3 – 5.



Obr. 3 – 5 Sekcia monitorovania v prípade zaznamenania útoku

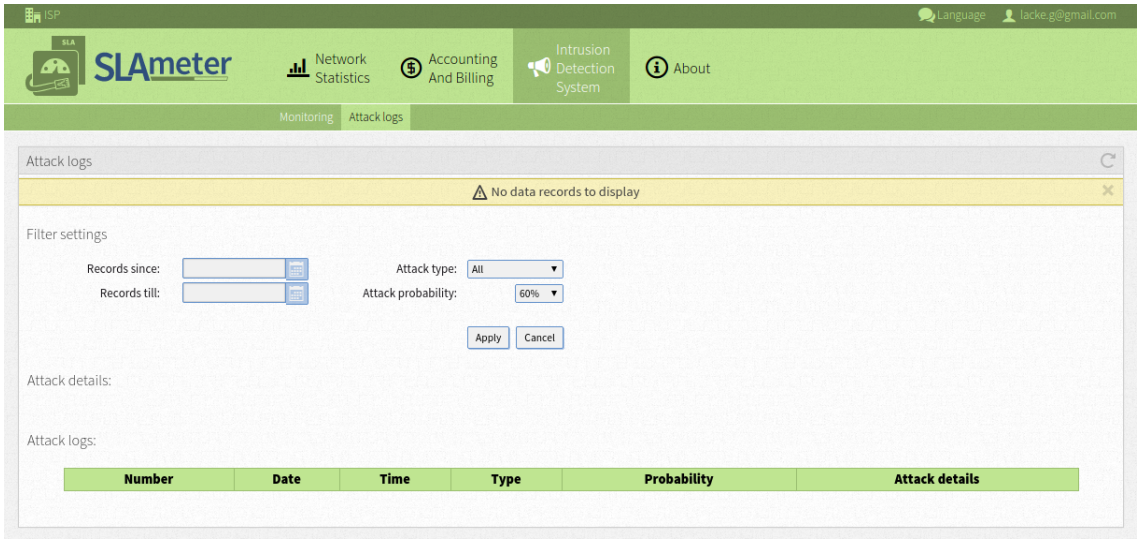
3.2.2 Záznamy o podozrivej prevádzke

Kliknutím na položku *Attack logs* sa v aplikácii ids zobrazí sekcia záznamov útokov. Webová aplikácia sa pripojí na databázový server a používateľovi zobrazí záznamy o podozrivej prevádzke za posledných 24 hodín. Ak žiadne záznamy pre daný čas nie sú uložené v databáze, pre používateľa sa zobrazí správa s upozornením (Obr. 3 – 6). V hornej časti sekcie *Attack logs* sa nachádza sekcia s filtrovacími kritériami, pričom záznamy o útokoch je možné filtrovať podľa:

- ***čas výskytu útoku*** – je možné zvoliť časové obdobie z ktorého majú byť vybrané záznamy, predvolené obdobie je posledných 24 hodín

- ***typ útoku*** – je možné určiť, ktoré typy útokov majú byť zobrazené, predvolená hodnota *all* zahŕňa všetky typy (*PortScan*, *SynFlood*, *UdpFlood*, *RstFlood*, *TtlFlood*, *FinFlood*)
- ***pravdepodobnosť útoku*** – určuje, že sa zobrazia záznamy o útokoch ktorých pravdepodobnosť výskytu bola vyhodnotená nad touto hodnotou, predvolená a minimálna hodnota je 60%, pretože bmIDSanalyzer zaznamenáva do databázy údaje o prevádzke s pravdepodobnosťou útoku nad 60% (túto hodnotu je však možné zmeniť v konfiguračnom súbore)

Po vyplnení filtračných kritérií treba aplikovať filter kliknutím na tlačidlo *Apply*. V prípade potreby vynulovania filtra sa použije tlačidlo *Cancel*, ktoré nastaví filtračné parametre na predvolené hodnoty, a údaje o záznamoch sa opäť načítajú za posledných 24 hodín.



Obr. 3 – 6 Sekcia *Attack logs*

Pod filtrom sekcie *Attack logs* sa nachádza sekcia pre zobrazenie detailných informácií o vybranom útoku, a pod touto sekciou je zobrazená tabuľka so záznamami útokov. Táto tabuľka obsahuje iba základné informácie o útokoch, ako dátum, čas, typ a pravdepodobnosť útoku. Pre zobrazenie detailnejších informácií o konkrétnom útoku je potrebné kliknúť na položku *Click to show details*, ktorá sa nachádza v

poslednom stĺpci tabuľky. Po kliknutí na túto položku sa nad hlavnou tabuľkou zobrazia detailné informácie o vybranom útoku. Sekciu po zobrazení detailných informácií o FIN záplavovom útoku zobrazuje obrázok Obr. 3 – 7.

Attack details:

FIN flood attack details:

Date:	14-04-2015, Tuesday
Time start:	21:45:54
Time end:	21:46:45
Source IP address:	192.168.1.93
Destination IP address:	192.168.1.102
FIN count:	25368
Probability:	100%

Since	Till	Count	Probability
21:45:54.00	21:45:58.00	2546	100%
21:45:59.00	21:46:03.00	2376	100%
21:46:04.00	21:46:08.00	2756	100%
21:46:09.00	21:46:13.01	2644	100%
21:46:14.01	21:46:18.01	2732	100%
21:46:19.01	21:46:24.00	3008	100%
21:46:25.01	21:46:30.01	2152	100%
21:46:31.01	21:46:35.01	2218	100%
21:46:36.01	21:46:40.02	2466	100%
21:46:41.02	21:46:45.13	2470	100%

Obr. 3 – 7 Sekcia s detailnými informáciami o FIN záplavovom útoku

4 Popis konfiguračného súboru

Pre aplikáciu bmIDSanalzer existuje konfiguračný súbor z ktorého pri spustení načíta potrebné údaje pre svoj správny beh. Sú to údaje pre pripojenie k databázovému serveru, pre pripojenie sa ku kolektoru, k SMTP serveru a obsahuje aj údaje pre samotný analyzér. Pre používateľa umožňuje upravenie týchto údajov podľa potreby. Súbor je zapísaný vo formáte XML, je jednouchý a ľahko čitateľný. Zoznam konfigurovateľných parametrov s ich popisom je uvedený v tabuľkách Tab. 4 – 1 a Tab. 4 – 2.

Tabuľka 4 – 1 Zoznam konfigurovateľných parametrov

Parameter	**Popis**
IDS settings	
threshold	prahová hodnota miery podozrenia, ktorej prekročenie signalizuje útok
Database setting - údaje k databáze ktorú používa kolektor	
ip	IP adresa databázoveho servera Postgresql
port	port na ktorom beží databázový server
name	názov databázy s používanymi tabuľkami
login	prihlasovacie meno k databáze
password	prihlasovacie heslo k databáze
ACP setting	
ip	IP adresa servera na ktorom beží kolektor
port	port na ktorom čaká kolektor pre pripojenie analyzéra
user	meno pre pripojenie ku kolektoru
password	heslo pre autentifikáciu ku kolektoru

Tabuľka 4 – 2 Zoznam konfigurovateľných parametrov (pokračovanie)

Parameter	**Popis**
Mail setting	
sendMail	voliteľné parametre sú *true* a *false*, pri konfigurácii *true* je posielanie emailových správ, v prípade detekovani útoku, zapnuté, pri konfigurácii *false* vypnuté
mailFrom	emailový účet aplikácie bmIDSanalyzer
mailFromPwd	heslo k emailovému účtu aplikácie bmIDSanalyzer
mailTo	emailový účet používateľa, na tento účet budú posielané emailové notifikácie v prípade útoku
SLAweb database setting - údaje k databáze ktorú používa webová aplikácia SLAmeter	
ip	IP adresa databázoveho servera Postgresql
port	port na ktorom beží databázový server
name	názov databázy s používanymi tabuľkami
login	prihlasovacie meno k databáze
password	prihlasovacie heslo k databáze
Standard traffic values	
portScan	štandardné hodnoty charakteristík pre útok skenovanie portov
synFlood	štandardné hodnoty charakteristík pre SYN záplavový útok
udpFlood	štandardné hodnoty charakteristík pre UDP záplavový útok
rstFlood	štandardné hodnoty charakteristík pre RST záplavový útok
ttlFlood	štandardné hodnoty charakteristík pre TTL záplavový útok
finFlood	štandardné hodnoty charakteristík pre FIN záplavový útok

5 Chybové hlásenia

Táto kapitola obsahuje iba niektoré chybové hlásenia systému bmIDS. Celkový zoznam chybových hlásení je možné nájsť v príručkách systému bmIDS (pozri referenciu).

5.1 Chybové hlásenia v aplikácii bmIDSanalyzer

Pri spustení programu alebo počas jeho behu môžu vzniknúť chyby. Program ich vypisuje na konzolu aj s detailným opisom. Najbežnejšie chybové hlásenia sú:

Chyba:
There is problem with mail server autentification. Please check config file.
Popis a riešenie:
Takéto chybové hlásenie signalizuje, že aplikácii bmIDSanalyzer sa nepodarilo vytvoriť spojenie s mail serverom.
Je potrebné skontrolovať, údaje v konfiguračnom súbore.

Chyba:
There is problem to start Redis server.
Popis a riešenie:
Chybové hlásenie signalizuje, že spustenie servera Redis bolo neúspešné. Je potrebné skontrolovať nastavenia systému.

5.2 Chybové hlásenia vo webovej aplikácii

V prípade výskytu chýb vo webovej aplikácii je používateľ upozornený programom nasledujúcimi chybovými hláseniami:

Chyba:

Unspecified error while loading data from server

Popis a riešenie:

Táto správa sa zobrazí v sekcii *Attack logs* keď nastane chyba pri načítavaní dát zo servera. Je potrebné skontrolovať pripojenie a pokúsiť sa o opätovné načítanie dát.

Literatúra

[1] UJLAKY, M.: *Systém bmIDS pre detekciu narušenia v počítačových sieťach*, Diplomová práca, Príloha B, KPI FEI TU, Košice, 2012.

[2] DEMČÁK, D.: *Systém pre detekciu narušenia založený na architektúre IPFIX*, Bakalárska práca, Príloha B, KPI FEI TU, Košice, 2012.

[3] ZÁVADA, V.: *Systém pre detekciu narušenia siete založený na IPFIX*, Bakalárska práca, Príloha B, KPI FEI TU, Košice, 2009.

[4] JUHÁR, J.: *Webová aplikácia nástroja SLAmeter*, Diplomová práca, Príloha B, KPI FEI TU, Košice, 2014.

[5] BERTA, L.: *Systémy pre detekciu narušenia sietí*, Bakalárska práca, Príloha B, KPI FEI TU, Košice, 2013.