DETECTING DOS AND DDOS ATTACKS USING NETFLOW DATA

Jan Huňka
Bachelor Degree Programme (4), FIT BUT
E-mail: xhunka01@stud.fit.vutbr.cz

Supervised by: Petr Matoušek
E-mail: matousp@fit.vutbr.cz

Abstract: This paper describes an implementation and challenges encountered during the process of designing a plugin for DoS and DDoS attacks detection on a FlowMon probe using NetFlow data. A detection method using correlation between transfered packets, flows and bytes is proposed. The method is applied on the plugin at the FlowMon probe. The plugin is tested on a reference ISCX dataset and experimental results are provided.

Keywords: DoS, DDoS, NetFlow, FlowMon, network attacks

1 ÚVOD

S rostoucím nebezpečím útoků typu Denial of Service (DoS) a jejich distribuovaných variant (DDoS) je stále potřebnější tyto útoky co nejrychleji detekovat a adekvátně na ně reagovat.

Tato práce vzniká ve spolupráci s brněnskou společnosti INVEA-TECH, která nabízí portfolio produktů FlowMon pro efektivní monitorování počítačových sítí na bázi síťových toků (NetFlow). Řešení FlowMon ovšem postrádá nástroj, který by zákazníky informoval o probíhajících útocích DoS a DDoS. Cílem je vytvořit plugin pro sondu FlowMon, který by na úrovni exportéru pomocí síťových toků dokázal detekovat nejpoužívanější typy těchto útoků a oznámil správci sítě IP adresy útočníků.

2 TVORBA PLUGINŮ PRO EXPORTÉR SONDY FLOWMON

Plugin je testován pomocí virtuální sondy FlowMon. Samotná aplikace se skládá z těchto čtyř dílčích pluginů, které společně tvoří požadovanou funkcionalitu:

- **Vstupní plugin**: Zachytává pakety a vytváří z nich NetFlow záznamy, které ukládá do rychlé paměti NetFlow cache. Zde je možné pracovat pouze s jednotlivými pakety.
- **Procesní plugin**: Umožňuje pracovat s jednotlivými toky při jejich vytvoření, modifikaci a expiraci. Zároveň jde o jediné místo, kde lze přistupovat k aktuálním tokům.
- **Filtrovací plugin**: Definuje filtry pro expirované toky, které rozhodují jejich exportu.
- **Exportní plugin**: Vytváří pakety s NetFlow záznamy a odesílá je na kolektor.

3 NÁVRH A IMPLEMENTACE DETEKCE

Útoky DoS a DDoS se využívají pro vyčerpání veškerých zdrojů cíle útoků. Může jít o výpočetní výkon, přenosové pásmo nebo omezení datových struktur operačního systému. Společným faktorem ale je, že se vždy projeví abnormálním počtem paketů, toků nebo velikostí přenesených dat. Mezi nejpoužívanější útoky patří UDP flood, SYN flood, ICMP flood a útoky na aplikační vrstvě jako HTTP flood [4]. Právě na tyto útoky a zejména jejich distribuované varianty jsem se zaměřil.

Diplomová práce Matěje Plcha z ČVUT [1] se zabývá závislostmi mezi počtem přenesených paketů, toků a bytů a na základě nich provádí detekci útoků DoS a DDoS na úrovni kolektoru. Je zde dokázáno, že v běžném provozu existuje mezi těmito metrikami přímá závislost. Při útoku je ale porušena, což může být použito jako zajímavá a obecná metoda detekce různých typů útoků.

V této práci navrhuji plugin exportéru sondy FlowMon, který by využil korelace mezi těmito metrikami pro detekci útoků DoS a DDoS. Exportér má oproti kolektoru k dispozici pouze aktuální provoz a je zde potřeba dbát na co nejmenší zpoždění detekce útoků.

K vyjádření korelace mezi metrikami x a y využívám Pearsonův korelační koeficient [3]. Proměnné x a y mohou nezávisle na pořadí reprezentovat jakékoliv dvě metriky z trojice pakety, toky, byty. Výpočet koeficientu pro sérii naměřených hodnot 1..n je definován následovně:

$$r = \frac{\sum_{i=1}^{n} [(x_i - \bar{x})(y_i - \bar{y})]}{\sqrt{\sum_{i=1}^{n} (x_i - \bar{x})^2 \sum_{i=1}^{n} (y_i - \bar{y})^2}}$$

Rovnice 1: Vzorec Pearsonova korelačního koeficientu

Hodnoty $\bar{x}$ a $\bar{y}$ značí střední hodnoty x, y v měřeném vzorku. Korelační koeficient nabývá hodnotu z intervalu <-1;1>, která určuje míru závislosti mezi metrikami. Při běžném provozu se jeho hodnota blíží k jedné, což značí přímou závislost. Při útoku se jeho hodnota snižuje k nule. Testováním se stanoví prahová hodnotu pro určení útoku.

Samotná detekce probíhá ve dvou fázích:

1. **Detekce probíhajícího útoku**: Na úrovni procesního pluginu se pro všechny toky společně načítají hodnoty počtu paketů, toků a bytů za jednu sekundu provozu po dobu časového okna (1-2 minuty). Po uplynutí časového okna se z nasbíraných metrik vyhodnotí korelační koeficienty a podle nastavené prahové hodnoty se rozhodne, zda probíhá útok. Jako rozšíření zvažuji možnost sběru metrik zvlášť pro protokoly TCP, UDP a ICMP. To by sloužilo k zpřesnění typu útoku.

2. **Detekce IP adres útočníků**: Ke zjištění konkrétních útočících IP adres bohužel nejsou k dispozici data z NetFlow cache, a proto využívám vlastní paměť typu hash tabulka. Do té se pro každou zdrojovou IP adresu ukládají pouze počty paketů, toků a bytů po délku časového okna. Navíc se ukládá počet jednopaketových toků s příznakem SYN pro detekci útoků SYN flood.

   Pokud je pomocí korelačních koeficientů odhalen probíhající útok, z hash tabulky se vyberou IP adresy přesahující stanovenou prahovou hodnotu a s dalšími informacemi jsou zapsány do logovacího souboru.

4 PRAKTICKÉ VÝSLEDKY

V tabulce 1 lze vidět korelační koeficienty dat nasbíraných během jednoho časového okna o délce 2 minuty. Během této doby se v datech objevila část HTTP flood útoku na aplikační vrstvě. Z výsledných korelačních koeficientů jde vidět, že lineární závislost je porušena ve dvojících pakety/toky a byty/toky. To značí, že počet toků v naměřeném vzorku nekoresponduje s nárůstem počtu paketů a bytů. V grafech na obrázcích 1-3 jsou jasně vidět místa, kdy došlo k razantnímů nárůstu počtu paketů a bytů, ale počet toků zůstal na normální hladině. Objevily se tedy toky, které obsahují abnormální počet paketů a přenáší velké množství dat k zahlcení cíle útoku.

Pokud je hodnota jednoho z koeficientů pod zadanou prahovou hodnotou, předpokládá se, že je v aktuálním časovém okně útok. Testováním se dále zjistí, jak se jednotlivé útoky promítají do korelačních

koeficientů, což pomůže při určování typu útoku.

Bylo tedy odhaleno porušení lineární závislosti mezi metrikami a útok byl úspěšně detekován. Plugin zároveň poskytl seznam dvou IP adres, které se v tomto krátkém časovém úseku účastnily útoku. Podle dokumentace testovacích dat bylo ověřeno, že se tyto adresy útoku opravdu účastnily.

Použitý záznam síťového provozu byl získán od organizace ISCX [2], která poskytuje referenční datasety síťového provozu s útoky pro výzkumné skupiny.

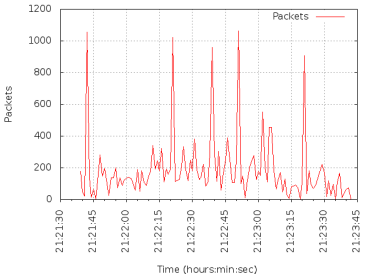
Metriky	Korelační koeficient
pakety/toky	0.146780
byty/toky	0.010568
byty/pakety	0.976237

Tabulka 1: Naměřené korelační koeficienty provozu s HTTP DDoS útokem

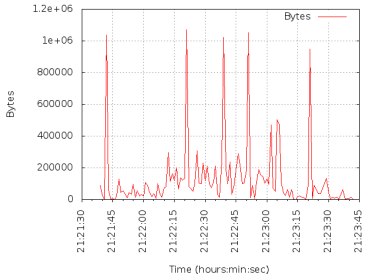
Metriky	Korelační koeficient
pakety/toky	0.956962
byty/toky	0.932944
byty/pakety	0.993384

Tabulka 2: Naměřené korelační koeficienty provozu bez útoku

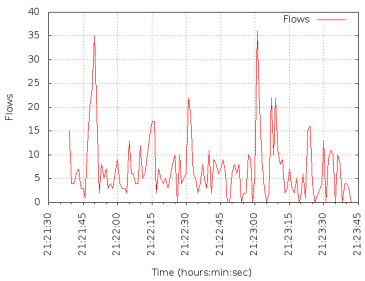
V tabulce 2 jsou pro porovnání uvedeny korelační koeficienty při běžném provozu bez útoku. Ty se blíží k 1, což znamená, že je zachována lineární závislost a nedošlo k žádnému útoku.



Obrázek 1: Počet paketů



Obrázek 2: Počet bytů



Obrázek 3: Počet toků

5 ZÁVĚR

V rámci této práce vznikl plugin pro sondu FlowMon, který bude pomocí změn v korelaci mezi pakety, toky a byty detekovat útoky DoS a DDoS. Hlavní výhodou tohoto řešení se při dosavadním testování ukázalo, že metoda dokáže obecně detekovat různé typy útoků. Nezaměřuje se totiž na vlastnosti procházejících dat, ale zabírá provoz jako celek a vyvozuje mezi ním statistické závislosti. Plugin musí samozřejmě projít rozsáhlým testováním, aby se určily spolehlivé prahové hodnoty detekce a zajistila se dostatečná rychlost pro nasazení na reálné síti. Testování bylo zatím úspěšně provedeno s provozem bez útoků a s provozem obsahujícím HTTP flood a SYN flood útoky. Zbývající typy útoků budou otestovány po získání relevantních testovacích dat.

REFERENCE

[1] Plch Matěj: Detekce DoS útoků pomocí analýzy síťových toků. DP 2012, FIT ČVUT.

[2] Shiravi A., Shiravi H., Tavallaee M., Ghorbani A.: Toward developing a systematic approach to generate benchmark datasets for instrusion detection. Computers & Security, 2012.

[3] Fajmon B., Koláček J.: Pravděpodobnost, statistika a operační výzkum. Elektronické skriptum FEKT VUT, 2005.

[4] Raghavan S.V., Dawson E.: An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks. Springer, 2011, ISBN 978-81-322-0276-9.