VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2017 Samuel Bronda

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

LABORATORNÍ ÚLOHA SEZNAMUJÍCÍ STUDENTY SE SYSTÉMY PREVENCE PRŮNIKŮ
LABORATORY TASK DEMONSTRATES INTRUSION PROTECTION SYSTEM

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Samuel Bronda**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Zdeněk Martinásek, Ph.D.**
SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní obor **Teleinformatika**
Ústav telekomunikací

Student: Samuel Bronda ***ID:*** 173620
Ročník: 3 ***Akademický rok:*** 2016/17

NÁZEV TÉMATU:

Laboratorní úloha seznamující studenty se systémy prevence průniků

POKYNY PRO VYPRACOVÁNÍ:

Hlavním cílem práce je navrhnout a vypracovat laboratorní úlohu seznamující studenty s principem IDS/IPS (Intrusion Detection/Prevention Systems) systémů. Prostudujte současný stav problematiky, nainstalujte a zprovozněte nejméně dvě volně dostupná řešení (např. SNORT nebo SURICATA) a nakonfigurujte detekce vybraných útoků (nejméně 5 vybraných typů DDoS o různých silách). Porovnejte detekční popřípadě mitigační schopnosti zprovozněných systémů a zaměřte se na diskuzi uživatelského rozhraní a visualizaci činnosti systémů. Navrhněte a vypracujte laboratorní úlohu seznamující studenty se základní instalací a konfigurací IDS/IPS cílené na DDoS (vyberte jednu implementaci).

DOPORUČENÁ LITERATURA:

[1] STALLINGS, William. Cryptography and network security: principles and practice. Seventh edition. 731 pages. ISBN 01-333-5469-5.

[2] CASWELL, Brian; BEALE, Jay. Snort 2.1 intrusion detection. Syngress, 2004.

Termín zadání: 1.2.2017 ***Termín odevzdání:*** 8.6.2017

Vedoucí práce: Ing. Zdeněk Martinásek, Ph.D.
Konzultant:

doc. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Táto bakalárska práca je rozdelená na dve časti. Teoretická časť popisuje zabezpečovacie systémy, rôzne druhy útokov a podrobne rozoberá systémy na ochranu počítačovej siete. Praktická časť je zameraná na pracovisko, na ktorom bude fungovať IDS/IPS systém Snort a Suricata, ich potrebným nastavením a simuláciou útokov. Bakalárska práca obsahuje aj nasadenie systému do reálnych podmienok.

KĽÚČOVÉ SLOVÁ

bezpečnosť, DoS, IDS, IPS, kontrola, sieť, Snort, Suricata útok, útočník

ABSTRACT

This bachelor thesis is divided into two parts. The theoretical part describes security systems, various types of attacks and details of systems to protect computer networks. The practical part focuses on the workplace, where will operate IDS / IPS system Snort and Suricata, the necessary adjustments and simulation of attacks. The bachelor thesis also includes putting the system into real terms.

KEYWORDS

attack, attacker, DoS, checking, IDS, IPS, network, security, Snort, Suricata

BRONDA, Samuel *Laboratórna úloha zoznamujúca študentov so systémami prevencie prienikov*: bakalárska práca. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikácií, 2016. 53 s. Vedúci práce bol Ing. Zdeněk Martinásek, Ph.D.

VYHLÁSENIE

Vyhlasujem, že som svoju bakalársku prácu na tému „Laboratórna úloha zoznamujúca študentov so systémami prevencie prienikov“ vypracoval(a) samostatne pod vedením vedúceho bakalárskej práce, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor(ka) uvedenej bakalárskej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto bakalárskej práce som neporušil(a) autorské práva tretích osôb, najmä som nezasiahol(-la) nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý(-á) následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákoníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autora(-ky)

POĎAKOVANIE

Rád by som poďakoval vedúcemu semestrálnej práce pánovi Ing. Zdenkovi Martinásekovi, Ph.D. za odborné vedenie, konzultácie, trpezlivosť, podnetné návrhy k práci.

Brno . . . .

podpis autora(-ky)

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic
http://www.six.feec.vutbr.cz

POĎAKOVANIE

Výzkum popsaný v tejto bakalárskej práci bol realizovaný v laboratóriách podporených projektom SIX; registračné číslo CZ.1.05/2.1.00/03.0072, operačný program Výzkum a vývoj pro inovace.

Brno . . . . . .

. . . . . .
podpis autora(-ky)

OBSAH

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ÚVOD

Cieľom bakalárskej práce je vytvoriť laboratórnu úlohu pre študentov na získanie nových vedomostí ohľadom IDS/IPS systémov. Táto úloha bola zvolená na základe vlastného záujmu o túto problematiku a z dôvodu získania nových vedomostí v danej téme. Výsledkom bude pripravená laboratórna úloha pre študentov v laboratórnom cvičení.

Bakalárska práca bude zameraná na teoretický rozbor problematiky, vytvorenie pracoviska na virtuálnych strojoch a nastavenie systémov, tak aby spĺňali naše požiadavky na laboratórnu úlohu.

Ochrana počítačovej siete alebo rôznych serverov je v dnešnej dobe veľmi náročná. Technológie sa veľkou rýchlosťou vyvíjajú, avšak aj útočníci prichádzajú vždy s novšími útokmi, ktoré majú za úlohu zistiť súkromné informácie zo siete, poškodiť siete, prípadne znemožniť prístup na servre. Na tieto útoky sa poväčšine používajú vírusy, spyware, spam a ine. S narastajúcim množstvom počítačovej siete a komunikácie v nej sa zvyšuje aj ohrozenie jednotlivých používateľov Internetu.

Možnosti ochrán je v dnešnej dobe niekoľko, k jednoduchým nástrojom patria rôzne meniace sa heslá a kódy, Anti-víry a Anti-spyware nachádzajúce sa koncových zariadeniach. Ďalší nástroj na obmedzenie komunikácie je Firewall. Medzi pokročilejšie nástroje patria IDS/IPS systémy, ktoré sa riadia pomocou definovaných pravidiel a dokážu nám lepšie, nie však úplne zabezpečiť sieť alebo server. Tento systém sleduje sieť a na základe definovaných pravidiel vie podniknúť istú reakciu na potencionálny útok alebo nebezpečenstvo.

Pracovisko bakalárskej práce bude realizované na počítači, kde budú nainštalované virtuálne stroje s operačným systémom Debian 8 Jessie zapojené v jednej sieti. Pracovisko poskytnuté školou slúži na prezentáciu reálnych výsledkov práce. Debian, je Linuxová distribúcia vhodná na to, aby jeden stroj slúžil ako webový server, ďalšie s nainštalovanými vybranými IDS/IPS systémami, ako ochrana a jeden útočník. Útočník sa pomocou rôznych útokov pokúsi obmedziť alebo znemožniť prevádzku servera.

Počítačový útočníci a útoky bývajú rôzne. Niektoré majú za úlohu len odpočúvať komunikáciu, iné majú znemožniť službu servera na niekoľko hodín. Niekedy ide aj o rozsiahle útoky vírusom, ktorý napadne niekoľko miliónov počítačov a zariadení. Záleží to od dôvodu a cieľa útočníka.

IDS/IPS systémy, ktoré budú použité v bakalárskej práce, sú Snort a Suricata. Ide o najrozšírenejšie systémy voľne prístupné na dnešnom trhu. Tieto systémy budú v závere bakalárskej práce porovnané.

1 POČÍTAČOVÝ ÚTOČNÍK A ÚTOK

Počítačový útočník je osoba alebo skupina, ktorá má na útok rôzne dôvody a ciele. Útok je akýkoľvek pokus nelegálne použiť počítačovú techniku.[1]

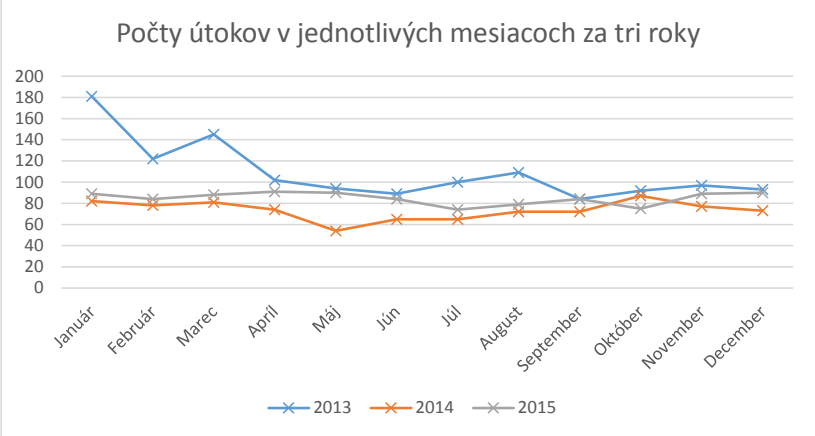
1.1 Počítačový útočník

Počítačová technika sa veľmi rýchlo vyvíja a aj počítačový útočníci sú viac a viac kreatívnejší. Žiaden systém nie je neprekonateľný, ak sa vymyslí nový typ zabezpečenia, útočníci vždy vymyslia nový spôsob jeho obídenia, prípadne znefunkčnenia. Podľa cieľu útoku útočníkov delíme na hackerov a crackerov. Obyčajný pracujúci človek, ktorý má záľubu v problematike vírusov, útokov a pod, no v žiadnom prípade nechce uškodiť počítačovej sieti sa nazýva hacker. Cracker je však odborník v problematike a svoje útoky robí z vlastného profitu, či už finančného alebo získavania dôležitých informácií.[1]

1.2 Počítačový útok

V počítačovej terminológií je útok akýkoľvek pokus poškodiť, zmeniť, ukradnúť majetok alebo sa nelegálne dostať pomocou cudzieho majetku do počítačovej siete alebo techniky. Počítačové útoky sú v dnešnej dobe obľúbenejšie, lebo aj pomocou nich sa útočníci vedia dostať ku finančnej alebo informačnej odmene a oveľa horšie je ich vypátrať ako pri bežnej lúpeži, keďže sa môžu napríklad skryť za inú IP adresu alebo pomocou vírusu vylákať peniaze od používateľov vírusom napadnutého počítača. Útoky môžeme rozdeliť na aktívne útoky, ktoré menia systémové prostriedky alebo ovplyvňujú ich chod a pasívne útoky, ktoré nemajú vplyv na systémove prostriedky, ale sa len využívajú na zber informácií zo systému. Útoky môžu byť realizované z vnútra alebo z vonku počítačovej siete. Každý počítačový útok je vyhodnotený ako trestný čin, tzn. hrozí odňatie slobody.[1]

O všetkých počítačových útokoch ľudia ani len netušia. Dozvedia sa iba o útokoch na veľké spoločnosti, ktoré boli zverejnené v médiach alebo útok pocítili vo firme, v ktorej pracujú. Na grafe 1.1, vidíme koľko útokov sa v jednotlivých mesiacoch v rokoch 2013, 2014 a 2015 uskutočnilo. V grafoch sú zobrazené iba útoky, ktoré boli zverejnené.[2]



Obr. 1.1: Graf zobrazujúci počty útokov v jednotlivých mesiacoch za posledné roky

1.2.1 Typy útokov

Existujú rôzne typy útokov a každý môže mať iný účinok. Vzhľadom na to, čo chce útočník dosiahnuť, útoky delime na:

- útoky na fyzický prístup
- útoky na skenovanie portov
- útoky na prevádzku služby
- útoky na účty rôznych typov
- útoky na chybu v systéme

Všetky útoky nemusia byť účinné, pretože v ich úlohe im často bránia bezpečnostné systémy.[3]

Graf 1.2 je znázorňuje percentuálne využitie typu útokov v roku 2015. Ako bolo spomenuté, útočníci vymýšľajú stále nové útoky, preto je veľa z nich pre bežný svet ešte nepoznaných.[2]

Obr. 1.2: Graf zobrazujúci percentuálny použitie druhu útoku

SQL Injection

Structured Query Language, je štruktúrovaný databázový jazyk používaný pre prácu s dátami. Príkazy SQL slúžia na aktualizovanie, získavanie alebo odoberanie dát z databáz. Základné príkazy jazyka sú select, ktorý slúži na vybratie. Insert slúži na vloženie. Pomocou príkazu update aktualizujeme. Prikáz delete vymaže záznam v tabuľke a príkaz drop tabuľku. Príkazom create sa tabuľka vytvorí.

SQL Injection patrí medzi jeden najhorších útokov. Tento útok sa používa poväčšine na získanie údajov z veľkých databáz. Ide o vloženie alebo priloženie aplikácie do databázy. Táto aplikácia má v sebe príkazy, ktoré sú odovzdané SQL serveru. Vtedy je celý server ohrozený. Aplikácia sa zlúči pomocou príkazov ku SQL a všetky dáta sú útočníkovi prístupne.[4]

Defacement

Defacement je veľmi nebezpečný útok na webovú službu. Defacement je útok, ktorý zmení obsah webovej stránky, a tak na oficiálnych stránkach dôležitého webu, sa môže vyskytnúť niečo nečakané. Väčšinou takýto útok vzniká na stránkach dvoch strán, kde jedna môže poškodiť druhú škodlivým obsahom, môže ísť o politické, teroristické alebo konkurenčné záujmy.

Za takýto útok sa dá považovať aj falošná webová stránka, ktorá vyzerá presne tak, ako oficiálna stránka napr. internet banking. Útočník žiada o zadanie prístupových údajov na svoju stránku, a ak si to používateľ nevšimne, útočník tak získa prístupové údaje.[5]

DoS

Denial of Service je útok, ktorý sa snaží o preťaženie niektorej služby množstvom požiadaviek. DoS útok prichádza z jedného zariadenia pomocou istého programu, pokiaľ je snaha zhodiť väčšie servere, a využíva sa pri tom viacero zaradení, ide o tzv. Distributed Denial of Service DDoS. Typy DoS útokov môžu byť rôzne a opäť záleží od cieľa útoku.[3]

SYN flood

Pri tomto útoku je potrebné si uvedomiť, ako funguje nadviazanie spojenia pomocou TCP. Počítač pošle TCP paket s príznakom “SYN“ (žiadosť o komunikáciu). Cieľový počítač odpovedá príznak “SYN“ a “ACK“ (pripravený na komunikáciu) a zdrojový počítač odpovedá zas “ACK“ (začneme komunikovať). Útočník požaduje komunikáciu, no ako zdrojová adresa v “ SYN“ pakete je zadaná iná, nedostupná IP adresa, cieľový počítač sa potom snaží nadviazať komunikáciu s nedosiahnuteľnou

adresou, pokiaľ nevyprší čas. Ak útočník zašle veľa “SYN“ paketov, vyčerpá sa tak pamäť na TCP spojenia.[3]

UDP flood

UDP flood útok, kde posielame UDP pakety s vymyslenou adresou odosielateľa. UDP nenadväzuje spojenie ako TCP. Útočník posiela pakety na náhodné porty cieľového počítača, ktoré nevyužívajú aplikácie. Počítač zašle ICMP paket s chybou. Pri dostatočnom množstve UDP paketov zdvojnásobíme prevádzku na sieti a počítač zamrzne.[3]

Zahltenie linky

Na cieľový server sa posiela veľké množstvo paketov, napr. ICMP ECHO. Server začne na každú žiadosť odpovedať, a tak dôjde k zahlteniu linky.[3]

Ping of death

Útok, ktorý využíva ICMP pakety a spočíva v zaslaní príliš veľkých ICMP ECHO paketov, ktoré zaplnia pamäť na cieľovom počítači.[3]

Hacknutie účtu

Tento druh útok nie je len o nastavení systému, ale aj o používateľoch, ktorí nie sú poučení o správnej ochrane svojich hesiel. Heslo sa môžu útočníci pokúsiť získať cez falošné emaily, prípadne prezradeným hesla v správach a pod.

Takéto heslo sa taktiež dá získať jeho uhádnutím pomocou prístupných crackovacích programov, prípadne použiť metódu „hrubej sily“(brute-force attack). Jednoduchým spôsobom, ako zistiť heslo na nešifrovanej sieti, je pomocou programu na sledovanie sieťovej prevádzky. Pokiaľ ide o koax alebo o hub, ktokoľvek môže odpočúvať prevádzku.[3]

2 BEZPEČNOSTNÉ SYSTÉMY IDS/IPS

Sú to systémy, ktoré nám pomáhajú s bezpečnosťou počítačovej sieti. Voľným prekladom hovoríme o systéme, ktorý nám deteguje prieniky na sieti, a zároveň aj urobí potrebnú prevenciu, aby im zabránil.

Tento systém monitoruje aktivitu na počítačovej sieti alebo samotnú aktivitu operačného systému. IDS/IPS vo veľkej miere zabraňuje útočníkom vykonať svoj útok na sieť alebo server.[6]

2.1 Intrusion Detection Systems

Intrusion (z ang.)znamená vnik, po preložení hovoríme o systéme na detekciu vniknutia. Ide o softvérovú aplikáciu, ktorá sleduje a monitoruje sieťový tok na sieti. Sieť monitoruje pomocou detekčných schopností, ktoré budú bližšie popísané ďalej v bakalárskej práci. Tento systém však nedokáže zabrániť útoku, tzn. vyšle nám iba alarm o podozrivej aktivite. Môžeme si to predstaviť ako alarm v obchode, ktorý varuje, že objekt bol narušený, ale nijako nevie zabrániť lúpeži.[6][7]

Pri vytváraní nového systému, je dôležité vopred si stanoviť, či sa bude jednať o systém jednovláknový alebo viacvláknový a tiež to, kde bude umiestnený a ako bude kontrolovať tok. Kontrola sieti je veľmi náročna a do úvahy je treba brať všetky aspekty.[8]

2.2 Intrusion Prevention Systems

Môžeme povedať, že ide o rozšírený Intrusion Detection System. Tento systém vie okrem základnej detekcie urobiť aj potrebné opatrenia, aby zabránil útoku v sieti alebo útok na server. IPS oproti IDS jedná samostatne, tzn., že kým IDS čaká, čo spraví administrátor siete, IPS rieši problém, napr. zastavenie komunikácie zo zdrojovej adresy potencionálneho nebezpečenstva, takáto jednoduchá činnosť sa dá spraviť aj pomocou IDS spolu s Firewall-om. IPS však musí byť nakonfigurovaná veľmi presne, aby sa obmedzili falošné poplachy, ktoré v prípade IDS vie správca označiť za falošné, IPS môže falošnými poplachmi narobiť veľké škody. Pre lepšiu predstavivosť si môžme predstaviť v obchode strážneho psa, ktorý po spustení alarmu vybehne za zlodejom.

IPS systémy poskytujú kompletnú kontrolu sieťových vrstiev. Medzi jeho operácie na prevenciu siete patrí:

- Posielanie alarmov administrátorovi
- Zahadzovanie nežiaducich paketov

- Blokovanie komunikácie zo zdrojov adresy
- Obnovovanie spojenia

[7]

2.3 Detekčné metódy

2.3.1 Stavová detekcia značiek

Ide o značky, ktoré sa nachádzajú v databáze. IDS/IPS systém hľadá v paketoch zhodu s paketmi, ktoré sú v databáze, kvôli tomu že niesli škodlivý obsah. Škodlivý obsah sa nemusí niesť iba v jednom pakete, ale môže byť rozložený aj do viacerých a systém je schopný ich spojiť a rekonštruovať. Databázy nie sú však vždy aktuálne, keďže útočníci vymýšľajú stále nové možnosti útoku.[6][7]

2.3.2 Odhalenie tokových anomálií

IDS/IPS systém sa vie učiť. Učí sa sieťový tok a podmienky, ktoré bežne vznikajú na sieti. Tieto podmienky si ukladá ako vzor, podľa ktorého sa riadi. Ak je tento vzor nejakým spôsobom porušený, systém vykoná príslušnú reakciu na hrozbu.[6][7]

2.3.3 Odhalenie protokolových anomálii

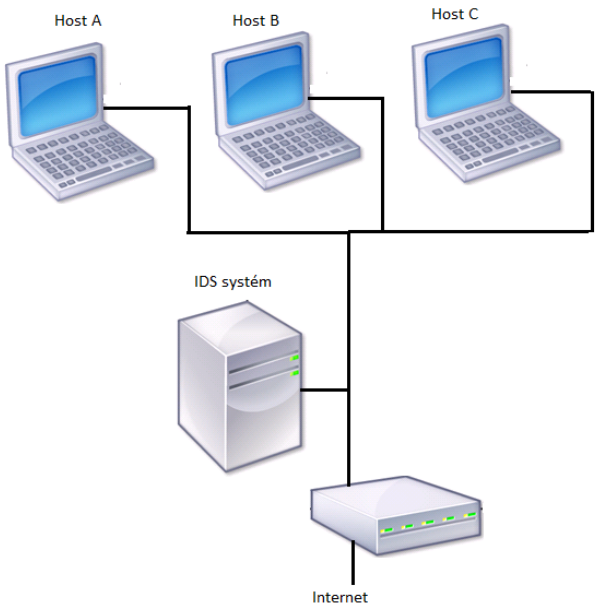
Sieťový tok má preddefinované svoje profily, tieto profily ma systém v sebe a na základe ich odchýlok vie detegovať útok a vykonať príslušnú reakciu.[6][7]

2.4 Rozdelenie podla umiestení v sieti

IDS systém sa môže umiestniť na rôzne miesta v sieti, podľa miesta inštalácií programu ich teda delíme do troch skupín. Každá z nich má svoje výhody aj nevýhody. Každú možnosť nasadenia systému je potrebné premyslieť podľa svojej úlohy, ktorú má plniť.[6][7]

2.4.1 Network-based Intrusion Detection System(NIDS)

Umiestenie je na najfrekventovanejšom mieste na sieti, tak aby bola zaistená kontrola celého toku dát do sieti. Pri tomto umiestnení nám vznikajú dva dôležité problémy. Toto umiestenie pracuje na sieťovej vrstve, takže možnosť analyzovať šifrované dáta nie je. Druhým problémom sú prepínané siete. Sondy musia byť umiestnené na vhodných miestach, aby monitorovali celý segment, najlepšie smerovač alebo most.[6][7]



Obr. 2.1: Ukážka Networt-based Intrusion Detection System

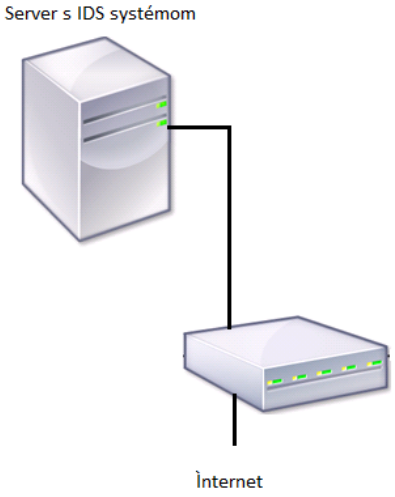
2.4.2 Hosted-based Intrusion Detection System(HIDS)

Umiestnenie je na úrovni hostiteľského systému, teda na používateľskej stanici alebo na serverovom počítači. Toto umiestnenie je predovšetkým zamerané na kontrolu tohoto zariadenia. IDS/IPS systém je väčšinou softvérová záležitosť, preto je dôležitý aj použitý operačný systém, aj keď väčšina programov funguje na všetkých platformách len s rozdielnym prístupom konfigurácii a prostredia. Keďže je na hostiteľskej úrovni rozumie, ako systém reaguje a funguje. Pracuje na úrovni aplikačnej vrstvy, takže dokáže sledovať aj šifrovanú komunikáciu.

Údržba takto umiestneného systému je náročná, nedá sa spraviť na všetkých uzloch naraz, ale treba ju robiť postupne na každom jednom. V prípade úspešného napadnutia napr. DoS útokom nastáva skutočný problém, pretože je napadnutý aj uzol, ktorý začne spracovávať nevhodné dáta.[6][7]

Honeypot

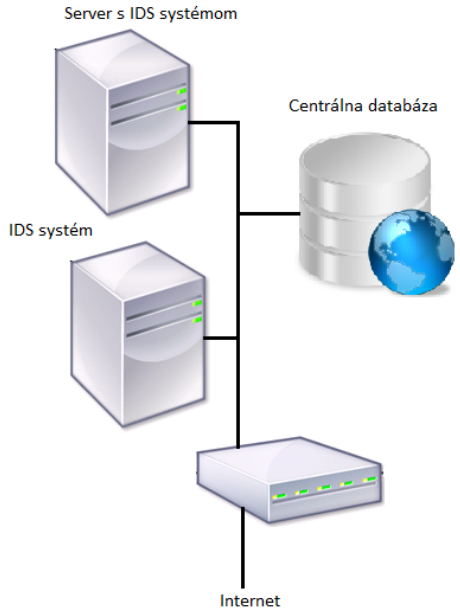
Pri HIDS ale aj celkovo pri IDS/IPS systémoch, naša sieť sa vie rozšíriť o Honeypot. Ide o informačný systém, ktorý pre svoju vlastnú IP adresu a dáta, ktoré obsahuje predstavuje ľahkú korisť pre útočníka. Honeypot toto presne chce, tým odhalí malware a môže ho analyzovať a poslať napríklad antivírusovým spoločnostiam, aby im vedeli zabrániť. IDS/IPS systém s kombináciu Honeypotu vie rýchlo a efektívne zabrániť útoku útočníka.[9]



Obr. 2.2: Ukážka Hosted-based Intrusion Detection System

2.4.3 Distributed-based Intrusion Detection System(DIDS)

DIDS koncept, ktorý zahŕňa obidva vyššie popísané umiestnenia. Systém je umiestnený v sieti aj na koncovom uzle. Všetky výsledky sa spracúvajú v centrálnej stanici. Toto riešenie zahrňuje všetky výhody NIDS a HIDS.[6][7]



Obr. 2.3: Ukážka Distributed-based Intrusion Detection System

2.5 Open Source IDS/IPS systémy

Open Source, v preklade otvorený zdroj, je systém, ktorého zdrojový kód so všetkými právami, je voľne prístupný na kopírovanie, používanie pre rôzne štúdie, zmeny a distribúciu pre kohokoľvek a za akýmkoľvek účelom.

Open Source systémy nebývajú drahé a veľmi často sú poskytované zadarmo. Tieto zdroje pomáhajú ušetriť ľudom niekoľko miliónov dolárov za drahé softvéry.

Tieto systémy sú vyvíjané z niekoľkých nezávislých zdrojov, systémy sú oveľa pestrejšie, napr. na dizajne, z toho dôvodu, že keď softvér vyvíja firma nerozvíja ho vo veľkej miere, a tak nie je udržateľný dlhodobo.

Tieto systémy často bývajú na oficiálnych stránkach voľne stiahnuteľné a takéto Open Source systémy budu použité v bakalárskej práci.[10][11]

2.6 Snort

Medzi najlepšie voľne prístupné programy typu IDS/IPS patrí na internete Snort. Tento systém dáva všetky potrebné informácie na zistenie sieťového útoku. Inštalácia tohoto, ale aj iných programov nie je vôbec jednoduchá, aj preto ho sprevádza kompletná dokumentácia. Snort nepotrebuje pravidelné aktualizácie, vylepšovanie a komplexný vývoj. Snort dokáže fungovať takmer na všetkých operačných systémoch. Ako už bolo spomenuté, tieto systémy fungujú na základe pravidiel, vďaka týmto pravidlám užívateľ redukuje falošné poplachy a dokáže sa tak lepšie zamerať na určité útoky.Snort môže pracovať v niekoľkých režimoch.[10][12][14]

Packet sniffer

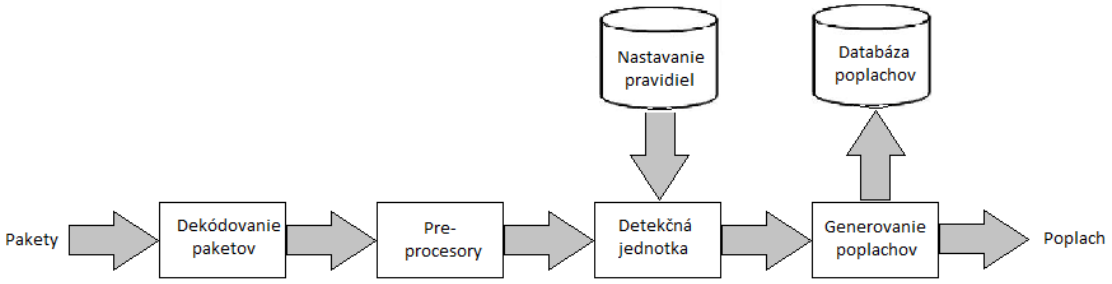
Pri tomto režime pracuje snort ako odposluch alebo sliedič. Výsledkom tohto režimu je výpis zachytávaných paketov rovno na obrazovku.[12]

Packet logger

Paket logger režim, ktorý je rozšírený oproti Paket snifferu o funkciu ukladania dát na disk.[12]

Network Intrusion Detection System

Snort pracuje na princípe definovaných pravidiel, podľa týchto pravidiel systém nezaznamenáva všetky pakety, ale pracuje na princípe analýzy. V tomto režime systém vyhodnocuje, ktoré pakety analyzuje. Na prechádzanie paketov môžeme doplniť Snort o zásuvné moduly.



Obr. 2.4: Snort zásuvne moduly

Zásuvné moduly slúžia na analýzu sieťového toku. K rozhodnutiu, či je potrebné paket analyzovať, slúži packet classifier. Rozhoduje, či ide o ethernetový alebo token ring rámec, UDP alebo TCP protokol a pod. Podľa toho je paket vyhodnotený ako potencionálne nebezpečný alebo neškodný, ak je nebezpečný je skenovaný detekčnou jednotkou.[14]

Na sieťovej vrstve prebieha analýza detekčnej jednotky, tá podľa definovaných pravidiel porovnáva pakety, napr. hľadá určitý obsah, anomáliu alebo kľúčové slová.

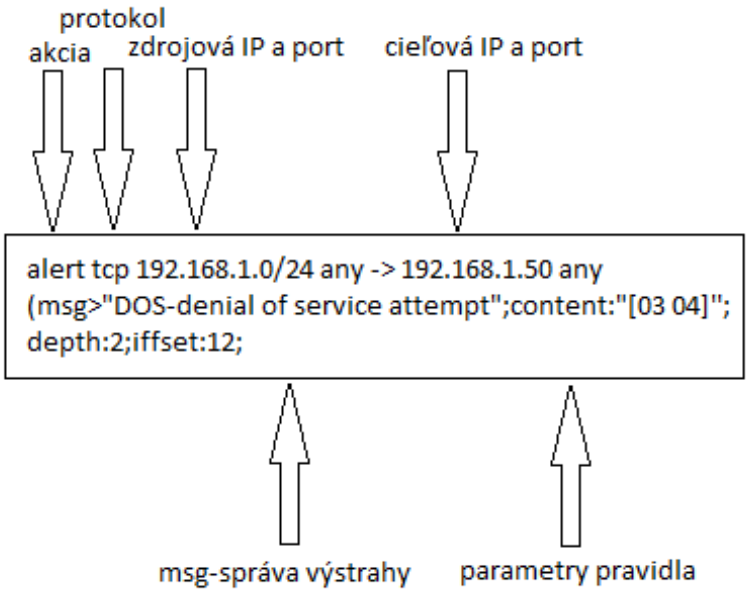
V detekčnej jednotke nájdeme tzv. IP defragmenter, ten rozdeľuje IP datagramy na menšie časti a potom ich skladá dokopy. Ide o jednoduchý dôvod, a to že datagramy nemusia prichádzať za sebou. Systém ich rozkladá a rozdeľuje podľa cieľa. Dobre navrhnuté systémy rozoznajú aj odosielanie datagramov z rôznych operačných systémoch.[14]

Modul, ktorý sa označuje ako stream5, skúma na úrovni transportnej už nie datagramy, ale segmenty. Skúmanie je podobné ako na sieťovej vrstve.

Na relačnej vrstve útočník analyzuje svoj cieľ. Môže na to využiť program NMap, pomocou ktorého zistí informácie o systéme, typy protokolov a dostupné porty. Aby nebol NMap nápadný, sfalšuje svoju IP adresu, ale systém Snort je na to pripravený cez preprocesor sfportscan.[12][13]

Pravidlá Snortu

Pravidlá Snortu sú uložené v textovom formáte v rôznych adresároch, záleží o aký typ pravidla ide. Ak ide o pravidlo typu File Transfer Protokol je uložené v adresári `ftp.rules`. Po spustení systému Snort sa vytvorí troj-dimenzovaný (3D) zoznam, ktorý slúži na detekciu paketov. Ukážka pravidla je na obr. 2.5[12][13]



Obr. 2.5: Ukážka Snort pravidla s popisom

Pravidlo sa skladá z hlavičky, ktorá obsahuje typ protokolu, zdrojovú adresu, port. Cieľovú adresu, port a hlavne udalosť, ktorá sa má stať s paketom, napr. upozorniť, zaznamenať, ignorovať, zahodiť a pod. Ďalej sa skladá z nastavenia tzv. tela, kde sú informácie, podľa ktorých je paket kontrolovaný, správa(informatívny obsah pre administrátora siete), kritéria a pod.[14]

Medzi akcie, ktoré dokážeme v pravidlách nastaviť patria:

- alert - akcia, ktorá vygeneruje správu s oznámením do konzoly. Výstraha upozorní administrátora siete a ten vykoná prípadnú reakciu. Je potrebné dať pozor na to, aby nedošlo k zahlteniu konzole, čo môže útočník využiť.
- log - uloženie paketu, slúži pre dôslednejšiu kontrolu. Ak si nie sme istí, či paket môže byť nebezpečný, paket sa uloží a môže byť skontrolovaní ďalšími nástrojmi.
- pass - veľmi jednoduchá akcia, ktorá povoľuje všetku komunikáciu podľa nastavení pravidla.
- activate - vzhľadom na to, že niekedy nie je jednoznačné, či sú veci nebezpečné alebo nie, je niekedy potrebné urobiť viacero krokov na odhalenie tejto komunikácie. Táto akcia sa sa dokáže obrátiť na inú akciu, ktorá o tom rozhodne.
- dynamic - čaká na aktiváciu od iného pravidla
- drop - akcia, ktorá zásadne ovplyvňuje tok dát na sieti. Nežiaduce pakety jednoducho zahodí a nepošlú sa ďalej, kde boli smerované. Malá časť sa uloží do logu. Paket môže byť zahodení jeden alebo viacero z daného spojenia. Pri tejto akcii je potrebné mať presne definované pravidlo, aby sme potrebné pakety

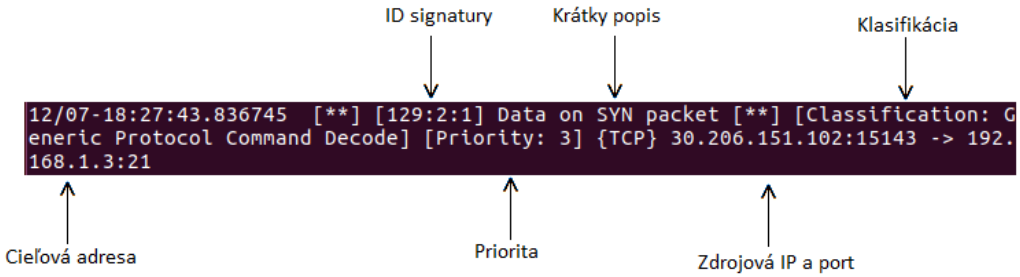
nemali zahadzované bez analýzy.

- reject - akcia blokovania komunikácie, paket uloží a resetne komunikáciu so zdrojom. Ak má systém podozrenie, že komunikácia môže byť nebezpečná.
- sdrop - ak vieme, že túto komunikáciu chceme maximálne filtrovať a nepotrebujeme o nej žiadne záznamy.

V jednoduchosti sa dá definovať aj vlastný typ pravidla.[12][13]

Výstraha Snortu

Keď paket príde a detekčná jednotka ho deteguje, naše pravidlo bolo nastavené na upozornenie, potom nám príde správa vo formáte na obr.2.6, kde môžeme vidieť aj popis časti výstrahy.



Obr. 2.6: Ukažka výstrahy po detekcií SYN paketov

DAQ

Data Acquisition library je knižnica, ktorá má priamo pracuje do libpcap. Slúži na riadenie vstupných a výstupných paketov. Typ DAQ záleži od našeho nastavenia systému Snort. Všetký typy sa nachádzajú v `/usr/local/lib/daq`.[14]

2.7 Suricata

Suricata je systém typu Open Source Next Generation IDS/IPS, tzn., že nejde o obyčajnú náhradu alebo vylepšenie existujúcich vecí, ale tento systém prináša nové technológie a nápady na zlepšenie zabezpečenia celej siete.

Suricata je ako Snort založená na pravidlách, pomocou ktorých monitoruje a kontroluje dátový tok do siete. Vyhodnocuje prichádzajúce pakety a na prípadné hrozby upozorňuje administrátora siete a vykonáva reakcie podľa pravidiel.

Tento systém beží na operačnom systéme Linux a je kompatibilný so všetkými existujúcimi sieťovými prvkami. Systém disponuje technológiu Multi-threading, čo

v analýze sieťového toku ponúka zvýšenie efektívnosti a rýchlosti práce, samozrejme s limitom hardvéru a sieťovej karty.[15]

Medzi hlavné nevýhody Suricaty oproti Snortu patrí dokumentácia, ktorá je väčšinou k dispozícii na ofic. str. oficiálnych stránok narozdiel od Snortu, o ktorom existuje veľa literárnych zdrojov, kníh, článkov a pod.[16]

Pravidlá Suricata

Pravidlá Suricaty sa dajú nastaviť na rôzne fungovanie. Pracujú na rôznych princípoch. Signatúry majú veľmi dôležitú úlohu. Veľa používateľov používa nastavené pravidlá, ktoré sa dajú upravovať, spravovať a majú stálu aktualizáciu. Každé pravidlo musí obsahovať `akciu, protokol, zdrojovú adresu, cieľovú adresu.`[16]

Meta-settings

Meta-nastavenie nemá hodnotu na funkčnosť Suricaty, ide skôr o informačnú hodnotu reportov. Nastavuje sa správa, ID signatúry, revízia, skupinové ID, zaradenie do skupiny, odkaz, priorita a metadata.[16]

Payload Keywords

Kľúčové slová komunikácie na sieti. Každý paket nesie o sebe správu. Payload Keywords analyzuje tok a hľadá v ňom klúčové slová. Ak by sme v pravidle nastavili content, teda obsah na hodnotu "snort", pakety, ktoré budú toto obsahovať nám budu dávať výstrahy.[16]

2.8 Ostatné IDS/IPS systémy

Vyššie spomenuté systémy patria medzi najpoužívanejšie, avšak poznáme ich ešte niekoľko.

Bro

Bro alebo niekedy známy aj ako Bro-IDS je takmer podobný systému Snort, či Suricata. Je založený na kontrolovaní značiek a anomálií. Celý tok konvertuje na udalosti, napr. prihlásenie na File Transfer Protokol, pripojenie na stránku a pod.

Po prevode na udalosti nám pomáha vlastný Bro-Script, ktorý má možnosť dodatku kontroly malware, čierne zoznamy zdrojov a pod.

Jeho nevýhodou je komplikované nastavenie. Medzi jeho výhody patrí detekcia niektorých vzorov, ktoré iné IDS nedetegujú, rozšírená architektúra a rast svojej komunity používateľov.[17]

Kismet

Kismet považujeme za základ Wireless IDS. Tento systém ukazuje svoju silu vo wireless protokoloch najmä 802.11. Najčastejšie hľadá neautorizované prihlásenie do siete a pracuje správne na všetkých platformách.[17]

OSSEC

OSSEC je IDS systém typu Host-based, je inštalovaný na hostoch, ktoré dáta posielajú na centrálny server, kde sa vyhodnocujú.

Veľkou výhodou OSSEC je jeho inštalácia, ktorá je veľmi jednoduchá a má veľkosť do 1MB, ostatné výhody sú: fungovanie na všetkých hlavných operačných systémoch a kompilovaný agent pre Windows.[17]

Samhain

Samhain je porovnateľný s systémom OSSEC, má rovnakú architektúru. Pri tomto systéme je treba dať pozor na správne výkonové nastavenie, ak sa nastaví príliš veľká rýchlosť, kontrola nebude dostatočná.

Má pomerne zložitú inštaláciu, ale je oveľa flexibilnejší.[17]

2.9 Grafický rozhranie pre IDS/IPS systémy

Jednou z častí zadania bakalárskej práce je uvažovať nad grafickým rozhraním systémov. Ako jednou z možností je Snorby. Ide o webovú aplikáciu, pre inú ľubovoľnú aplikáciu, ktorá posiela dáta v binárnom formáte na vstup Snorby, ktorý tieto dáta zobrazí. Snorby neslúži na ovládanie systémov, jeho úlohou je len zobrazovať binárne súbory. Všetky nastavenia systémov je potrebné vykonať pomocou konfiguračných súborov. Pomocou Snorby si vieme zobraziť rôzne grafy, udalosti a pod., ktoré sa stali v IDS/IPS systémov.[18]

2.10 Operačný systém Debian 8 Jessie

Hlavným operačným systémom celej bakalárskej práce je Debian 8 Jessie. Je to voľný operačný systém, vytváraný združením Debian Project. Jadro Debianu momentálne tvorí Linux alebo FreeBSD. Veľká časť nástrojov pochádza z projektu GNU. Debian je veľmi široko využiteľný software, dodáva sa s viac ako 43000 balíkov.

Debian nie je ale čisto slobodný software, existuje niekoľko balíkov, na ktoré je potrebné mať platenú verziu systému Debian.[19]

Prvé poznatky o Debiane prišli v roku 1993. the Debian Linux Release, nazval prvý systém muž menom Ian Murdock. Prvé verzie Debianu od 0,01 až po verziu 0,90 neboli pre verejnosť. Verzia 0,90 bola prvá, ktorá sa dostala na verejnosť a poskytovala podporu elektronickej pošte Pixar.[19]

Hardwarové požiadavky na systém sú doslova minimálne, a preto dokáže bežať od malých prenosných počítačov po veľké serverové systémy. Taktiež ma široké spektrum architektúry, na ktorých dokáže bežať.[19]

Operačný systém je preto veľmi výhodný a taktiež môže byť nainštalovaný na serveroch. V bakalárskej práci je použitý na všetkých zariadeniach vo virtuálnom stroji a na fyzickom zariadení filtri Mikrotik

3 IMPLEMENTÁCIA IDS/IPS SYSTÉMOV

Implementácia systémov bola realizovaná pomocou školských zariadení a virtuálnych strojov, ktoré budú slúžiť laboratórnej úlohe.

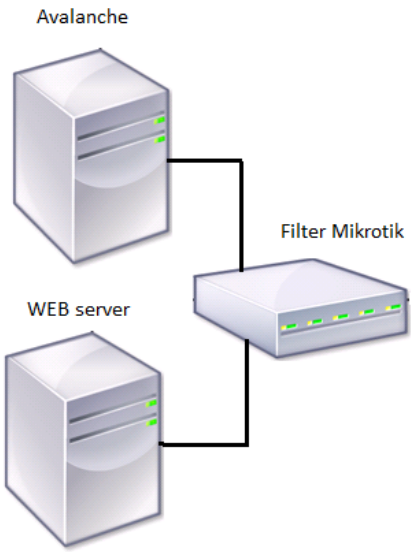
Systémy, ktoré sú použité v bakalárskej práci sú Snort a Suricata. Tieto systémy patria medzi najznámejšie. Suricata v dnešnej dobe veľmi prekvitá a za Snortom nezaostáva.

Pracovisko poskytnuté školou slúži na vytvorenie reálnejších podmienok nasadenia systému. Systém bežiaci na filtri prevádzky od firmy Mikrotik je Suricata. Je nastavený s vlastnými pravidlami na obranu pred útokmi SYN flood a UDP flood, generované pomocou serveru s nainštalovaným programom Spirent Test Center.

Systémy, s ktorými študenti budú pracovať v rámci laboratórnej úlohy sú Snort aj Suricata. Snort je nainštalovaný a študenti majú za úlohu jeho konfiguráciu. So Suricatou sa študenti zoznámia pri jej kompletnej inštalácii.

3.1 Fyzické pracovisko a výsledky

Fyzické pracovisko slúži ako podklad pre reálne hodnoty a prácu so Suricatou vzhľadom na to, že vo virtuálnych strojoch nedokážeme dosiahnuť vysokú prenosovú rýchlosť. Zjednodušená schéma zapojenia zariadení je na obr. 3.1. Na filtri je nainštalovaný IDS/IPS systém Suricata. Jeho kompletná inštalácia je v odseku 3.4.



Obr. 3.1: Zapojenie fyzického pracoviska

Editor na úpravu konfiguračných súborov

Na úpravu konfiguračných súborov je potrebné naučiť sa pár príkazov editora VIM alebo GNU nano. GNU nano je pomerne jednoduchší nástroj narozdieľ od editora VIM, ktorý je o niečo zložitejší no pokročilejší.

Tab. 3.1: Tabuľka základných skratiek programu GNU nano

Skratka	**Udalosť**
Ctrl + G	Otvorí pomocnú dokumentáciu
Ctrl + X	Zatvorenie súbru
Ctrl + O	Uloženie ako nový súbor
Ctrl + R	Vloží obsah z iného súboru
Ctrl + W	Vyhladavanie v súbore
Ctrl + Y	Predchádzajúca stránka
Ctrl + V	Nasledujúca stránka
Ctrl + K	Vystrihnutie textu
Ctrl + U	Zrušenie vystrihnutia textu
Ctrl + C	Aktuálna pozícia kurzora
Ctrl + T	Rozdeliť

Tab. 3.2: Tabuľka základných príkazov editora VIM

Príkaz	**Udalosť**
i	Písanie na pozícu kurzoza
:	Vyhladávanie riadku
wq	Uložiť a vypnúť
ESC	Zrušenie aktuálneho režimu
!q	Hrubé ukončenie editora

Nastavené pravidlá Suricaty

Pravidlá sú nastavené manuálne, tak aby zachýtavali útoky typu SYN flood a UDP flood, ktorý Avalanche dokáže generovať.

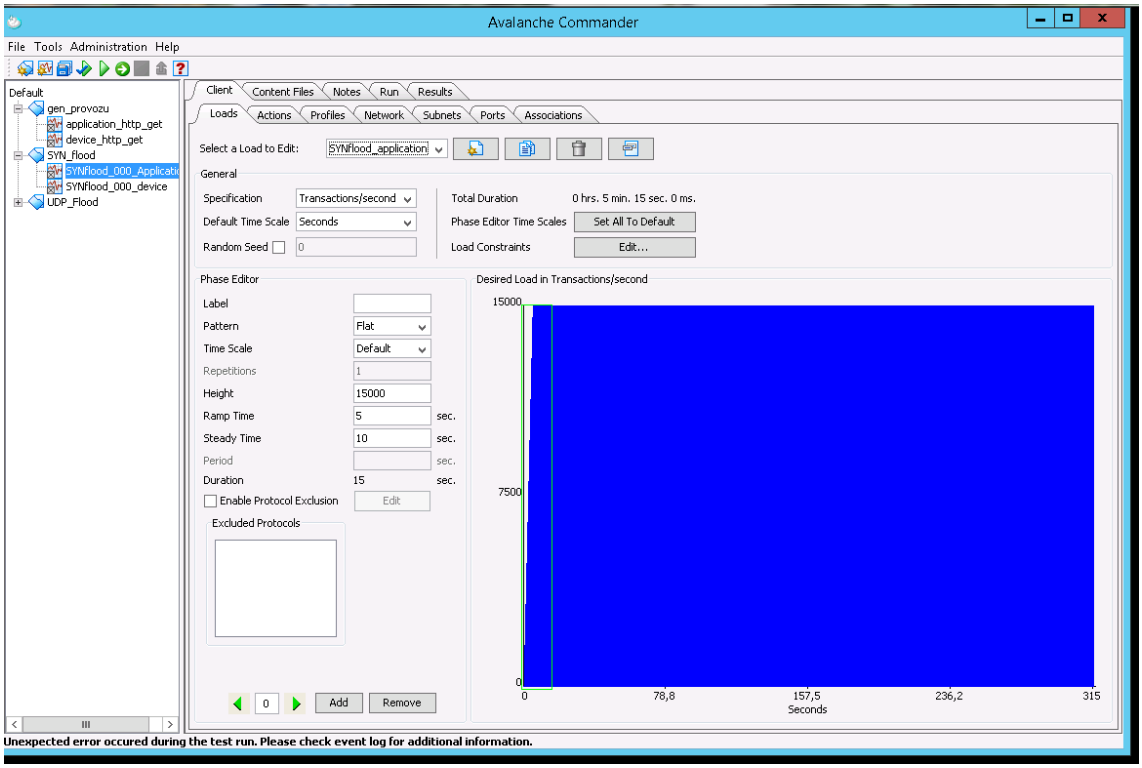
Jednoduché pravidla na detekciu paketov s protokolom UDP a TCP s označeím SYN.

Server Avalanche generoval pakety podľa nastavení. Na obr.3.3 sú nastavené transakcie za sekundu. Počet transakcií je 15000.

```
 GNU nano 2.2.6                File: /etc/suricata/rules/local.rules                Modified

alert tcp any any -> $HOME_NET any (msg: "Possible DDos attack, SYN flag detected"; flags: S; sid:1;gid:1;)
alert udp any any -> $HOME_NET any (msg: "Possible DDos attack, UDP flood"; sid:2; gid:2;)
```

Obr. 3.2: Vlastné pravidlá nastavené na filtri Mikrotik



Obr. 3.3: Ukážka nastavenia SYN flood útoku

Výsledky zachytávania útokov

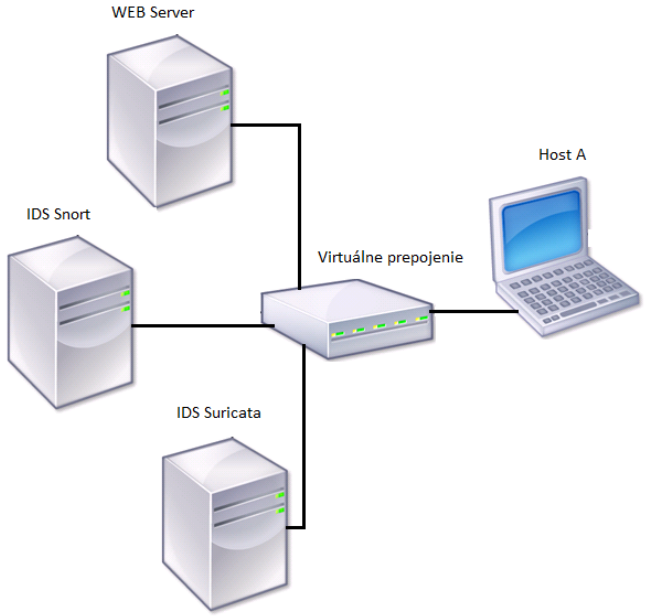
Jednotlivé pravidlá boli neskôr nastavené na akciu drop, v tom prípade nám každý jeden paket s označením SYN prípadne posielaný na protokole UDP bol zahodený. Pakety boli zachytávanie o rôznych silách. Začínalo sa od poslaných pár paketov s najmenšou veľkosťou až po veľa paketov z veľkou veľkosťou. Jednotlivé pakety boli zachytávané a alerty ukladáne do `fast.log`.

Niekoľko pokusov o vyradenie služby na webovom serveri boli neúspešných. Na vine bolo pravdepodobne zlé nastavenie servera Avalanche. Práca na fyzickom zariadení bola ale úspešná z dôvodu zachytávania útokov systémom Suricata o rôznych silách a veľkostiach.

Hlavnou výhodou prenosu na reálnych zariadeniach je prenosová rýchlosť, ktorá sa nedá dosiahnuť vo virtuálnom stroji. Realnejšie podmienky na hardwere filtre a pod.

3.2 Virtuálne pracovisko a výsledky

K zostaveniu virtuálneho pracoviska bude v laboratórnej úlohe je využitý vlastný počítač, na ktorom je nainštalovaný Oracle VM VirtualBox. VirtualBox obsahuje 4 virtuálne systémy typu Debian 8 Jessie 64 bitovej verzii. Zapojenie pracoviska je na obr. 3.4. Na serveri beží webová služba. IDS systémy Snort a Suricata sú v režime NIDS a Host A predstavuje útočníka.



Obr. 3.4: Zapojenie virtuálneho pracoviska

Virtuálne stroje majú nastavené dva sieťové adaptéri, jeden sieťový adaptér slúži na pripojenie k internetu a je nastavený v NAT režime. Druhý adaptér je pripojený do lokálnej sieťe, spojené sú pomocou virtuálneho prostredia. Nastavenie IP adries lokálneho spojenia je v tab.3.3.

Tab. 3.3: IP adresy pridelené virtuálnym strojom

Tabuľka IP adries vo virtuálnom prostredí	
IDS Snort	192.168.1.3
IDS Suricata	192.168.1.4
Host A	192.168.1.5
Web Server	192.168.1.254

Pre vyskúšanie dvoch rozličných variant som sa rozhodol, že Snort bude nainštalovaný s databázou MySQL a s automatickým nastavením pravidiel. Suricata

bude nastavená manuálne bez ďalších doplnkov. Pravidlá sú veľmi jednoduché a ich primárny účel je študentov naučiť ich obsah a syntax.

Testovanie systémov sa konalo pomocou paketového generátora hping3. Parametre používané pri generovaní paketov sú zobrazené v tab.3.4. Konkrétne príkazy na vybraný útok sú zobrazené v tab.3.5.

Tab. 3.4: Používané parametre príkazu hping3

hping3	
-2	UDP mód
-1	ICMP mód
-0	RAW IP mód
-c	počet paketov
-p	port
-d	veľkosť paketu
-S	nastavenie SYN označenia
–fast	10 paketov za sekundu
–flood	najrýchlejšie posielanie paketov

Tab. 3.5: Nastavenie príkazu hping3 na konkrétny útok

Generované útoky pomocou príkazu hping3	
SYN flood	hping3 -c 100000 -d 120 -S –flood 192.168.1.x
UDP flood	hping3 -2 –flood 192.168.1.x
HTTP flood	hping3 -c 100000 -d 50 -p 80 –flood 192.168.1.x
Ping of Death	hping3 -c 100000 -d 500 -p 20 -1 –flood 192.168.1.x
RAW IP paket	hping3 -c 100000 -d 8 -0 –flood 192.168.1.x

Webový server slúži ako cieľ napadnutia útoku, na virtuálnom stroji beží Apache2, kde je nastavená malá úvodná stránka. Slúži na reálnejšiu predstavu počítačovej siete.

Virtuálne pracovisko so systémom Suricata

Pravidlá nastavené v Suricate sú cielené na vybrané a častou používané DoS útoky. Na obr. 3.5 sú zobrazené pravidlá, ktoré som nastavil v systéme. Pravidlá sú nastavené ako upozornenia na potencionálne útoky typu: SYN flood, UDP flood, HTTP flood, Ping od Death a RAW IP pakety.

Jednotlivé útoky boli presne zadané do príkazového riadku Hosta A, ktorý simuluje útočníka. Systém Suricata sa spušta príkazom `suricata -c /etc/suricata/su`

```
  GNU nano 2.2.6              File: /etc/suricata/rules/local.rules

alert tcp any any -> $HOME_NET any (flags: S; msg:"SYNC detected"; sid:1;gid:1;)
alert udp any any -> $HOME_NET any (msg:"Possible UDP flood"; sid:2;gid: 2;)
alert tcp any any -> $HOME_NET 80 (msg:"HTTP connection"; sid:3; gid:3;)
alert icmp any any -> $HOME_NET any (msg:"Possible ping od death attack"; sid:4; gid:4;)
alert ip any any -> $HOME_NET any (msg:"IP paket";sid:5;gid:4;)
```

Obr. 3.5: Manuálne nastavenie pravidiel v Suricate

`ricata.yaml -i eth1 -init-errors-fatal` Všetky výstrahy sú nastavené aby sa zapisovali do `/var/log/suricata/fast.log`. Po vypísaní logovacieho súboru príkazom `cat /var/log/suricata/fast.log` sú zobrazené jednotlivé výstrahy útokov, podla definovaných pravidiel. Taktiež je možné sledovať aj `stats.log`, ktorý slúži na celkovú štatistiku paketov prechádzajúcich cez systém. `drop.log` služi na logovanie paketov, ktore boli zahodené systémom.

Jednotlivé výstrahy manuálne nastavené v local.rules sú na obrázkoch nižšie. Každá jedna výstraha obsahuje dátum, nastavené sid a gid, správu, prioritu a zdrojovú a cieľovú IP adresu.

```
05/30/2017-05:59:24.266508  [**] [1:1:0] SYNC detected [**] [Classification: (null)] [Priority: 3] {T
CP} 192.168.1.5:58763 -> 192.168.1.4:0
```

Obr. 3.6: Výstraha Suricata po SYN flood útoku

```
05/29/2017-16:15:35.225320  [**] [2:2:0] Possible UDP flood attack [**] [Classif
ication: (null)] [Priority: 3] {UDP} 192.168.1.5:8437 -> 192.168.1.4:0
```

Obr. 3.7: Výstraha Suricata po UDP flood útoku

```
05/30/2017-06:04:10.996954  [**] [3:3:0] HTTP connection [**] [Classification: (null)] [Priority: 3]
{TCP} 192.168.1.5:18929 -> 192.168.1.4:80
```

Obr. 3.8: Výstraha Suricata po HTTP flood útoku

```
05/29/2017-16:20:06.049846  [**] [4:4:0] Possible ping od death attack [**] [Cla
ssification: (null)] [Priority: 3] {ICMP} 192.168.1.4:0 -> 192.168.1.5:0
```

Obr. 3.9: Výstraha Suricata po Ping of Death útoku

```
05/30/2017-06:07:37.539885  [**] [4:5:0] IP paket [**] [Classification: (null)] [Priority: 3] {TCP} 1
92.168.1.5:0 -> 192.168.1.4:0
```

Obr. 3.10: Výstraha Suricata po IP RAW zaslaní paketov

Virtuálne pracovisko so systémom Snort

Systém Snort je nainštalovaný a pripravený do prevádzky pomocou automatických pravidiel stiahnutých z oficiálnych stránok. Taktiež systém bol doplnení o databázu MySQL a systémom PulledPork, ktorý sa stará o automatickú aktualizáciu pravidiel. Pri aktualizácii pravidiel je dôležité byť registrovaný na oficiálne stránky Snort. Po registrácii je pridelený oinkcode, bez ktorého sťahovanie snort pokročilejších pravidiel nie je možné.

Inštalácia systému Snort je popísaná v kapitole3.3. Spustenie systému PulledPork malo za následok pridanie viac ako 50 000 tisíc pravidiel a viac ako 20 000 nežiadúcich IP adries.

```
Rule Stats...
        New:-------0
        Deleted:---633
        Enabled Rules:----29534
        Dropped Rules:----0
        Disabled Rules:---26366
        Total Rules:------55900
IP Blacklist Stats...
        Total IPs:-----21217
```

Obr. 3.11: Počet pridaných pravidiel systémom PulledPork

Systém Snort sa taktiež testoval útokmi pomocou generátoru paketov `hping3`. Snort vyhlásil upozornenie pri SYN flood a HTTP flood, ostatné nepovažoval za nebezpečné, pravdepodobne z dôvodu nízkej prenosovej rýchlosti medzi virtuálnymi strojmi. Výstrahy, ktoré vidíme nižšie vygeneroval Snort.

```
06/06-14:25:50.346204  [**] [129:2:1] Data on SYN packet [**] [Classification
: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.1.5:6772 -> 19
2.168.1.3:0
```

Obr. 3.12: Výstraha Snort po zachytení SYN flood

```
06/06-14:28:16.923772  [**] [129:11:1] TCP Data with no TCP Flags set [**] [C
lassification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.1
.5:33005 -> 192.168.1.3:80
```

Obr. 3.13: Výstraha Snort po zachytení HTTP flood

Ak by sme nastavili manuálne pravidlá v `local.rules` pakety by určite zachytil aj Snort. Inštalácia, spojená s databázou MySql ukladá tieto dáta aj do databázy.

Snort by určite detegoval iné pakety vzhľadom jeho veľkým množstvám pravidiel. Všetky záznamy, ktoré sú nastavené v konfiguračnom súbore Snort sa ukladajú do logovacích súborov.

3.3 Popis inštalácie a nastavenia Snort

Inštalácia Snortu nie je náročná, avšak náročné je samotný Snort nastaviť. Nastavenie nebude vhodné na prevádzku v skutočnom nasadení, ale na splnenie úlohy pre študentov, ktorí sa zoznamujú so systémami IDS/IPS.

Systém bude nainštalovaný ako NIDS, má samostatné miesto v sieti, ktorú kontroluje.

Operačný systém pre server je Debian, ktorý musí byť pred samotnou inštaláciou Snort na to pripravený, na to sú potrebné nainštalované balíčky.

Pre uľahčenie práce s právami, všetky nasledujúce príkazy budú vykonané ako root. Na nastavenie a inštalácia Snortu sú potrebné doplnkové knižnice, ktoré sa nenachádzajú v základnom systéme. Sú to knižnice na správu sieťovej komunikácie.

```
apt-get install build-essential libpcap-dev libpcre3-dev libdumbnet
-dev -y
```

Nasledujúce príkazy slúžia na vytvorenie adresára pre stiahnutie, ide o archivovaný súbor, takže jeho rozbalenie a inštaláciu Snort. Čerpanie príkazov je z oficiálnych stránok Snortu. Obsahujú jeho minimálne nastavenie na fungovanie systému, nastavenie pravidiel a správu systému.

```
mkdir ~/snort_src
cd ~/snort_src
apt-get install bison flex -y
wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
tar -xvzf daq-2.0.6.tar.gz
cd daq-2.0.6
./configure
make
make install
cd ~/snort_src
apt-get install zlib1g-dev liblzma-dev openssl libssl-dev -y
wget https://www.snort.org/downloads/snort/snort-2.9.8.3.tar.gz
tar -xvzf snort-2.9.8.3.tar.gz
cd snort-2.9.8.3
./configure --enable-sourcefire
```

```
make
make install
```

Snort bol nainštalovaný, nasleduje jeho konfigurácia. Uvedené príkazy vytvárajú potrebné adresáre, kde budú uložené pravidlá. Adresáre, je potrebné, vytvoriť aby sa mali kde uložiť pravidla.

```
ldconfig
ln -s /usr/local/bin/snort /usr/sbin/snort
groupadd snort
useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort
mkdir -p /etc/snort/rules/iplists
mkdir /etc/snort/preproc_rules
mkdir /usr/local/lib/snort_dynamicrules
mkdir /etc/snort/so_rules
mkdir -p /var/log/snort/archived_logs
touch /etc/snort/rules/iplists/black_list.rules
touch /etc/snort/rules/iplists/white_list.rules
touch /etc/snort/rules/local.rules
touch /etc/snort/sid-msg.map
```

Nasledujú príkazy na kopírovanie konfiguračných súborov do dynamických preprocesorov.

```
cd ~/snort_src/snort-2.9.8.2/etc/
sudo cp *.conf* /etc/snort
sudo cp *.map /etc/snort
sudo cp *.dtd /etc/snort
cd ~/snort_src/snort-2.9.8.2/src/dynamic-preprocessors/build/usr/loc
al/lib/snort_dynamicpreprocessor/
sudo cp * /usr/local/lib/snort_dynamicpreprocessor/
```

V konfiguračnom súbore Snort je potrebné nastavenie domácej siete a nastavenie ciest k súborom pravidiel. snort.conf ponúka rozličné nastavenie systému. V konfiguračnom súbore je možnosť nastavenia veľmi veľa druhov pravidiel, veľa druhov výstupov, rozlične spôsoby logovania záznamov a fungovanie Snortu.

```
vim /etc/snort/snort.conf
```

Úprava údajov v konfiguračnom súbore

```
ipvar HOME_NET 192.168.1.0/24

var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules

var WHITE_LIST_PATH /etc/snort/rules/iplists
var BLACK_LIST_PATH /etc/snort/rules/iplists
```

Inštalácia Barnyard2

Barnyard2 je program, ktorý je potrebný na ukladanie dát do databázy. Snort generuje dáta v binárnej forme a Barnyard2 ich prekladá.

Nasledujúce príkazy popisujú inštaláciu, vytvorenie potrebných súborov a nastavenie Barnyard2. Pri inštalácii Barnyard2 je potrebné zvoliť si root heslo.

```
apt-get install mysql-server libmysqlclient-dev mysql-client autoconf
libtool -y
cd ~/snort_src/
git clone git://github.com/firnsy/barnyard2.git
cd barnyard2/
autoreconf -fvi -I ./m4
ln -s /usr/include/dumbnet.h /usr/include/dnet.h
ldconfig
./configure --with-mysql --with-mysql-libraries=/usr/lib/x86_64-linux
-gnu
make
make install
cp etc/barnyard2.conf /etc/snort
mkdir /var/log/barnyard2
chown snort.snort /var/log/barnyard2
touch /var/log/snort/barnyard2.waldo
chown snort.snort /var/log/snort/barnyard2.waldo
```

Všetky útoky, hrozby sa zapisujú do databázy, nasledujú príkazy na jej konfiguráciu. Barnyard2 má v sebe pred pripravenú schému databázu a tabuliek. Pri veľkých systémoch je jednoduchšie implementovať databázu, ktorá je jednoduchšia na správu a prácu s ňou.

```
mysql -u root -p
create database snort;
```

```
use snort
source ~/snort_src/barnyard2/schemas/create_mysql
CREATE USER 'snort'@'localhost'IDENTIFIED BY '**********';
grant create, insert, select, delete, update on snort.* to 'snort'@
'localhost';
```

Nastavenie práce Barnyard2 a MySql.

```
vim /etc/snort/barnyard2.conf
output database: log, mysql, user=snort password=********** dbname=
snort host=localhost
chmod o-r /etc/snort/barnyard2.conf
```

Inštalácia PulledPork

Pre čo najlepšie fungovanie pravidiel, a pri aktualizácii posledných pravidiel nám pomáha PullerPork. PulledPork je skript, ktorý aktualizuje a sťahuje nové pravidlá do systému Snort. Po nainštalovaní a spustení nám PulledPork pridal tisíce nových pravidiel, ktoré nám pomôžu zabezpečiť systém pred útokmi.

```
cd ~/snort_src/
wget https://github.com/finchy/pulledpork/archive/patch-3.zip
unzip patch-3.zip
cd pulledpork-patch-3
sudo cp pulledpork.pl /usr/local/bin/
sudo chmod +x /usr/local/bin/pulledpork.pl
sudo cp etc/*.conf /etc/snort/
```

Dokončenie konfigurácie PulledPork sa robilo v konfiguračnom súbore, kde sa upravovali cesty k pravidlám. Systém PulledPork je možné nastaviť aby sťahoval napr. len komunitné pravidlá, ktoré ale nie sú dostačujúce. Komunitné pravidlá sú dostupné aj bez registrácie. Po registrácií je užívateľovi pridelený oinkcode, ktorý dovoľuje sťahovať pokročilejšie pravidlá z oficiálnych stránok. Systém Snort ponúka ešte kvalitnejšie pravidla pre predplatiteľov.

3.4 Popis inštalácie a nastavenia Suricata

Inštalácia Suricata bude podobná ako inštalácia Snort, pôjde o takmer rovnaké príkazy s podobnou testovacou konfiguráciou. Celá inštalácia bude kvôli právomociam spracovaná pod root-om. Suricata je nainštalovaná na novom virtuálnom stroji, k jej inštalácii je potrebné doinštalovať knižnice. Príkazy na inštaláciu.

```
apt-get -y install libpcre3 libpcre3-dbg libpcre3-dev
build-essential autoconf automake libtool libpcap-dev libnet1-dev
libyaml-0-2 libyaml-dev zlib1g zlib1g-dev libmagic-dev libcap-ng-dev
libjansson-dev pkg-config
mkdir ~/suricata_src
cd ~/suricata_src
wget http://www.openinfosecfoundation.org/download/suricata-3.2.1.tar.gz
tar -xvzf suricata-3.2.1.tar.gz
cd suricata-3.2.1
./configure --enable-nfqueue --prefix=/usr --sysconfdir=/etc
--localstatedir=/var
./configure --prefix=/usr --sysconfdir=/etc/ --localstatedir=/var
make
make install
ldconfig
```

Suricata ponúka taktiež veľmi užitočnú inštaláciu s konfiguračnými súbormi. Suricata tým pádom vytvorí základnú konfiguráciu za nás a ušetrí nám veľa času. Taktiež ponúka automatickú inštaláciu Suricata pravidiel, ktoré ak sa nevyznáme v pravidlách, nám uľahčia robotu.

```
./configure && make && make install-conf
./configure && make && make install-rules
```

Vytvorenie potrebných adresárov. Adresár, ktorý je vytvorený v `/var/log/`slúži na oddelenie logov týkajúcich sa Suricaty od ostatných. V adresári `/etc/` má Suricata vlastný priestor, obsahuje všetký konfiguračné súbory systému Suricata. V adresári `/etc/suricata/rules` sa nachádzajú všetky pravidlá.

```
mkdir /var/log/suricata
mkdir /etc/suricata
mkdir /etc/suricata/rules
```

Kopírovanie konfiguračných súborov do adresárov. `classification.conf` slúži na klasifikáciu uchádzajúcich paketov. Aj na základe tejto hodnoty sa systém rozhoduje, či ide o nebezpečenstvo alebo nie. `reference.config` je konfiguračný súbor, ktorý obsahuje všetky pôvodné nastavenia systému.

```
cp classification.config /etc/suricata
cp reference.config /etc/suricata
cp suricata.yaml /etc/suricata
```

V systéme Suricata pre jeho správne fungovanie je potrebné spraviť pár zmien v jeho konfiguračnom súbore suricata.yaml. Suricata.yaml je veľký obsiahly súbor. Suricatu si dokáže prispôsobiť presne na svoje účely a ponúka veľmi veľa možností svojho fungovania.

```
nano /etc/suricata/suricata.yaml
address-groups: HOME_NET: "[192.168.1.0/24]"
default-rule-path"' /etc/suricata/rules
rule-files:
- local.rules (ostatné zakomentovať)
classification-file: /etc/suricata/classification.config
reference-config-file: /etc/suricata/reference.config
-drop:
alerts:yes
```

Konfiguračný súbor suricata.yaml je pripravený, potrebné je nastaviť lokálne pravidlá v súbore local.rules. Systém Suricata ponúka aj veľa iných pravidiel rôznych typov. Rôzne typy pravidiel sa oddeľujú do rôznych .rules priečinkov, veľkou výhodou tohoto delenia je spravovanie pravidiel. Ak mame pravidlo, ktoré sa týka malware, pridáme ho do malwere.rules a nebudeme ho hľadať medzi niekoľkými pravidlami napr. dos.rules.

```
nano /etc/suricata/rules/local.rules
```

Podobne ako pri Snorte je aj pri Suricate možné doinštalovať systém na aktualizáciu pravidiel, databázu MySQL a grafické rozhranie. Príkazy na to sú ale veľmi podobné.

3.5 Porovnanie systémov

Vlastnosti systémov

Dlhodobo je v popredí IDS/IPS systém Snort. Jeho dokumentácia správa systému, nastavenie a fungovanie je na veľmi dobrej úrovni. Mnoho ľudí dáva Suricatu až na druhé miesto prípadne nižšie. Momentálne sa Suricata ale rozrastá, jej oficiálne stránky sú na kompletnú prípravu systému viac ako dostačujúce. K dobrému menu Snortu prispie aj fakt, že je dostupný už takmer 20 rokov zatial čo Suricata ani nie 10 rokov.[20]

Systému sú kódované jazykom C. Suricata, ako poslednú stabilnu verziu na všetky platformi používa verziu 3.0. Snort používa verziu 2.9.8.3.[20]

Tab. 3.6: Porovnavanie vlastnosti systémov

	Snort	**Suricata**
Typ	jedno-vláknové	viac-vláknové
Dokumentácia	Dostatok materialov na internete, oficialna dokumentácia Snort	Dobrá oficiálna dokumentácia ale menej návodou na internete
Pravidlá	Komplexné oficiálne pravidlá + manuálne pravidlá	Komplexné oficiálne pravidlá + manuálne pravidlá
Podpora IPv6	Áno	Áno
Práca offline	Áno	Áno
Inštalácia(v mojom pohlade)	Pomerne jednoduchá inštalácia, zaleží od nastavenia celého systému a čo od neho očakávame	Jednoduchšia inštalácia a implementácia oficiálnych pravidiel ako Snort

Obidva systémy ponúkajú automatické aj manuálne nastavenie pravidiel. Najlepšou možnosťou je kombinácia týchto riešení vzhľadom na to, že tieto pravidlá spolu dokážu fungovať. Pri vytváraní nových pravidiel je potrebné byť veľmi opatrný, aby sme svoju sieť nezabezpečili úplne alebo v horšom prípade vôbec.[20]

Veľkou výhodou Suricaty je viac-vláknová práca, tým pádom sa procesor nemusí využívať na 100% ale svoj výkon dokáže rozdeliť.[20]

Obidva systémy sú vhodné na použitie vo veľkých aj malých firmách. Ak sa administrátori siete nevedia rozhodnúť, ktorý systém je ten lepší, nie je problém implementovať aj obidva systémy do siete.[20]

Hlavné výhody systému Snort sú:

- Škálovateľnosť - dokáže byť bezproblémovo nasadený do akejkoľvek sieti.
- Flexibilita a použiteľnosť - dokáže fungovať na väčšine operačných systémov.
- Naživo - v reálnom čase dokáže monitorovať počítačovú sieť.
- Rozšíriteľnosť - dokáže byť rozšírení o niekoľko druhov databázových systémov, logovacích systémov a dokáže byť rozšírený o rôzne nástroje.
- Rýchlosť - svoju prácu vykonáva veľmi rýchlo a tým pádom pomáha vo veľa prípadoch ostatným systémom sieti a tak zabraňuje nežiaducej komunikácii, vírusom a pod.
- Postavenie v sieti - v sieti dokáže byť postavený takmer kdekoľvek. Pred, za alebo dokonca vedľa firewallu.[20]

Hlavné výhody systému Suricata sú:

- Open Source Engine - komunitne vytváraný systém dokáže byť veľmi rastúci

a účinný. Ten prípad ukazuje aj Suricata.

- Viac - vláknový - pri viac jadrovom procesore dokáže oveľa rýchlejšie vykonávať svoju prácu a byť tým viac nápomocný.
- Automatická detekcia protokolov - Preprocesory automaticky identifikujú použité protokoly a tak na sieťový tok dokážu aplikovať nastavené pravidla.[20]

4 ZÁVER

Bakalárska práca bola zameraná na podrobnejšie oboznámenie sa s bezpečnostnými systémami IDS/IPS. Tieto systémy na rozdiel od bežných ochranných prvkov, ako sú firewall a anti-vírus, sledujú celé spektrum hrozieb, ktoré sa môže dostať do siete. Hlavným problémom týchto systémov je správne nastavenie pravidiel, aby nedochádzalo k falošným poplachom, ale aby boli splnené bezpečnostné zásady. Pokročilejšie systémy vyhodnocujú aktivity v sieti ako neškodné, potencionálne nebezpečné a nebezpečné a podľa vyhodnotenia aktivít vykonajú príslušná reakciu.

Bakalárska práca sa tiež venovala príprave laboratórnej úlohe pre študentov, aby nadobudli základné poznatky ohľadom bezpečnostných systémoch IDS/IPS. V úlohe sa študenti oboznámia s kompletnou inštaláciou systému Suricata a konfiguráciu systému Snort. Taktiež si vyskúšajú manuálne nastavenie pravidiel a automatické nastavenie z oficiálnych stránok systému.

Pri inštalácií systému Suricata do fyzického prostredia, nedošlo k veľkým zmenám oproti virtuálnemu prostrediu. Veľkou výhodou je výpočtová hodnota. Systém Suricata je viac vláknový systém a preto nedochádza k preťaženiu jedného procesora.

Systém Snort je považovaný za jeden z najlepších zabezpečovacích systémov. Systém Suricata sa ale veľmi rýchlo vyvíja a miestami sa tak dostáva do popredia. Dokumentácia systému začína byť prepracovanejšia a objavuje sa viac návodov a riešení problémov na internet.

Obidva systémy v bakalárskej práci boli nakonfigurované správne, vzhľadom na ich schopnosť útok detegovať a zahodiť nebezpečné pakety. Automatická aktualizácia pravidiel je veľmi jednoduchá a nenáročná, vhodná pre ľudí, ktorý nepoznajú správu počítačových sieti. Manuálne nastavenie môže byť o niečo presnejšie, ale zároveň je náročnejšie, na čas, vedomosti a aktualizáciu.

Bakalárska práca bola pre mňa prínosná ohľadom nových poznatkov bezpečností sieti, systémov IDS/IPS. Mojou prácou som vytvoril laboratórnu úlohu, ktorá naučí študentov základné a mierne pokročilejšie poznatky ohľadom týchto systémov.

LITERATÚRA

[1] JOHNSON, Thomas A. *Cybersecurity: protecting critical infrastructures from cyber attack and cyber warfare* 2015, [cit. 17. 10. 2016]. CRC Press., ISBN 9781482239225.

[2] PASSERI, Paolo. *2015 Cyber attacks statistics* [online]. 2016, [cit. 10. 10. 2016]. Hackmageddon. Dostupný z URL: <`http://www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics/`>.

[3] NORIS, Ivan. *Bezpečnosť servera v sieti* [online]. 2007, [cit. 9. 10. 2016].Dostupný z URL: <`http://deja-vix.sk/sysadmin/security.html#dos_network`>.

[4] CLARKE, Justin. *SQL Injection attacks and defense* 2009, [cit. 10. 10. 2016]. Syngress Publishing, Inc.,str.457., ISBN 9781597494243.

[5] VATIS, A. Michael. *Cyber attacks during the war on terrorism: A predictive analysis* 2001 , [cit. 10. 10. 2016]. INSTITUTE FOR SECURITY TECHNOLOGY STUDIES AT DARTMOUTH COLLEGE.

[6] RASH, Michael. *Intrusion prevention and active response: deploying network and host IPS*2005, [cit. 1. 11. 2016].Rockland, Mass.: Syngress Publishing., ISBN 193226647.

[7] HORÁK, Michal. *Jak mohou pomoci systémy detekce a prevence narušení* [online]. 2005, [cit. 9. 10. 2016]. Dostupný z URL: <`http://www.actinet.cz/pdf/ccbs-acti-clv-0512.pdf`>.

[8] CROTHERS, Tim. *Implementing intrusion detection systems: a hands-on guide for securing the network* 2003, [cit. 5. 4. 2016] Indianapolis, IN: Wiley Pub., ISBN 0764549499.

[9] SPITZNER, Lance. *Honeypots tracking hackers* 2002, [cit. 17. 11. 2016]. Addison-Wesley. ISBN 0321108957.

[10] SCOTT, Charlie., Paul. WOLFE a Bert. HAYES. *Snort for dummies.* 2004, [cit. 10. 11. 2016]. Hoboken, NJ: Wiley Pub., 0-337, ISBN 0764568353

[11] LAKHANI, Karim R. *How open source software works: "free" user-to-user assistance* 2002, [cit. 10. 11. 2016]. MIT Sloan School of Management, 50 Memorial Drive.

[12] ČÍŽEK, Zdeněk. *Snort jako open source etalon pro IPS* 2009, [cit. 10. 11. 2016]. Security World., č.1, str. 23. ISSN 1210-9924

[13] BEALE, Jay., James C.Foster. *Snort 2.0 Intrusion Detection* 2003, [cit. 14. 11. 2016]. Oxford: Elsevier Science, ISBN 1931836744

[14] *Snort Network Intrusion Detection & Prevention System* [online] 2017, [cit. 5. 1. 2017]. Dostupný z URL: <`https://www.snort.org/`>.

[15] LANG, Jean-Philippe. *Suricata User Guide* [online] 2016, [cit. 14. 11. 2016].Dostupný z URL: <`http://suricata.readthedocs.io/en/latest/#`>.

[16] *Suricata | Open Source IDS / IPS /NSM engine* [online] 2017, [cit. 5. 1. 2017]. Dostupný z URL: <`https://suricata-ids.org/`>.

[17] SCHREIBER, Joe. *Open Source Intrusion Detection (IDS) Tools: A Quick Overview* [online]. 2014, [cit. 14. 11. 2016].Dostupný z URL: <`https://www.alienvault.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview`>.

[18] ZINDILIS, Marios. *What and Why of Snorby* [online] 2015, [cit. 5. 3. 2017]. Dostupný z URL: <`https://github.com/Snorby/snorby/wiki/What-and-Why-of-Snorby`>.

[19] *Debian – Univerzálny operačný systém* [online] 2017, [cit. 5. 1. 2017]. Dostupný z URL: <`https://www.debian.org/`>.

[20] *Aanval - Snort, Suricata, and Syslog Intrusion Detection, Correlation and Threat Management* [online] 2017, [cit. 5. 5. 2017]. Dostupný z URL: <`https://www.aanval.com/`>.

ZOZNAM SYMBOLOV, VELIČÍN A SKRATIEK

ACK Acknowledge – Potvrdenie

DIDS Distributed-based Intrusion Detection System – Distribuvano založený systém prevencie prenikov

DoS Denial of Service – Vyradenie prevádzky služby

HIDS Hosted-based Intrusion Detection System – Na koncovom uzle založený systém prevencie prenikov

HTTP Hypertext transfer protocol – Hypertextový prenosový protokol

ICMP Internet Control Message Protocol – Protokol internetovej kontrolnej správy

IDS Intrusion Detection System – Systém detekcie prienikov

IP Internet Protocol – Internetový protokol

IPS Intrusion Prevention System – Systém prevencie prienikov

NIDS Network-based Intrusion Detection System – Sieťovo založený systém prevencie prenikov

RFC Request For Comments – Žiadosť o komentáre

SQL Structured Query Language – štruktúrovaný dopytovací jazyk

SYN Synchronize – Synchronizácia

TCP Transimission Control Protocol – Protokol riadenia prenosu

UDP User Datagram Protocol – Používateľský datagramový protokol

ZOZNAM PRÍLOH

A LABORATÓRNA ÚLOHA

Laboratorní úloha seznamující se systémy prevence průniků

Úloha:

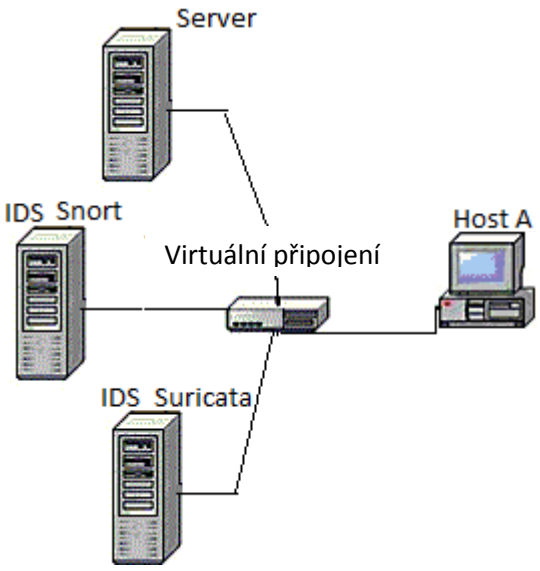
- Instalace a konfigurace systému Suricata
- Konfigurace systému Snort
- Detekce útoků

Teoretický rozbor:

IDS/IPS jsou systémy, které nám pomáhají s bezpečností počítačové sítě. Volným překladem mluvíme o systémech, které nám detekují průniky na síti a zároveň i provedou potřebnou prevenci, aby jim zabránily.

Tyto systémy monitorují aktivitu na počítačové síti nebo samotnou aktivitu operačního systému. IDS/IPS ve velké míře zabraňují útočníkům vykonat útok na síť nebo server. Fungují na principu pravidel.

Pracoviště:



Postup:

Tabulka IP adres	
IDS Snort	192.168.1.3
IDS Suricata	192.168.1.4
Host A	192.168.1.5
Web Server	192.168.1.254

Heslo pro uživatele a pro root je 123456.

Spusťte virtuální stroje a ověřte nastavení IP adres.

Každý virtuální stroj má dva síťové adaptéry, jeden je připojený do vnější NAT sítě a druhý je připojený do lokální sítě. Nastavení IP adres ověříte přikazem: ifconfig.

1. Otevřete terminál ve virtuálním stroji Suricata a přihlašte se jako root.

   Pomocí přiložených příkazů stáhněte, nainstalujte a nakonfigurujte systém Suricata.

   apt-get -y install libpcre3 libpcre3-dbg libpcre3-dev
   build-essential autoconf automake libtool libpcap-dev libnet1-dev
   libyaml-0-2 libyaml-dev zlib1g zlib1g-dev libmagic-dev libcap-ng-dev
   libjansson-dev pkg-config
   mkdir ~/suricata_src
   cd ~/suricata_src
   wget http://www.openinfosecfoundation.org/download/suricata-3.2.1.tar.gz
   tar -xvzf suricata-3.2.1.tar.gz
   cd suricata-3.2.1
   ./configure --enable-nfqueue --prefix=/usr --sysconfdir=/etc --localstatedir=/var
   ./configure --prefix=/usr --sysconfdir=/etc/ --localstatedir=/var
   make
   make install
   ldconfig
   Suricata nabízí taktéž velmi užitečnou instalaci s konfiguračními soubory a s pravidly.
   ./configure && make && make install-conf
   ./configure && make && make install-rules
   Vytvoření potřebných adresářů:
   mkdir /var/log/suricata
   mkdir /etc/suricata
   mkdir /etc/suricata/rules
   Kopírování konfiguračních souborů do adresářů:
   cp classification.config /etc/suricata
   cp reference.config /etc/suricata
   cp suricata.yaml /etc/suricata
   V systému Suricata pro jeho správné fungování je potřeba udělat pár změn v jeho konfiguračním souboru suricata.yaml.
   nano /etc/suricata/suricata.yaml
   address-groups: HOME_NET: "[192.168.1.0/24]"
   default-rule-path"’ /etc/suricata/rules
   rule-files:
   - local.rules (ostatné zakomentovať)
   classification-file: /etc/suricata/classification.config
   reference-config-file: /etc/suricata/reference.config
   -drop:
   alerts:yes
   Konfigurační soubor suricata.yaml je připravený, potřebné je nastavit lokální pravidla v souboru local.rules.
   nano /etc/suricata/rules/local.rules

Jak bylo zmíněno, systémy fungují na principu pravidel, tyto pravidla je možné psát manuálně nebo je stáhnout z oficiálních stránek.

```
  GNU nano 2.2.6              File: /etc/suricata/rules/local.rules

alert tcp any any -> $HOME_NET any (flags: S; msg:"SYNC detected"; sid:1;gid:1;)
alert udp any any -> $HOME_NET any (msg:"Possible UDP flood"; sid:2;gid: 2;)
alert tcp any any -> $HOME_NET 80 (msg:"HTTP connection"; sid:3; gid:3;)
alert icmp any any -> $HOME_NET any (msg:"Possible ping od death attack"; sid:4; gid:4;)
alert ip any any -> $HOME_NET any (msg:"IP paket";sid:5;gid:4;)
```

2. Nakonfigurujte systém Snort.

Nastavení v Snort.conf

:~$ sudo sed -i "s/include \$RULE_PATH/#include \$RULE_PATH/" /etc/snort/snort.conf

:~$ sudo vi /etc/snort/snort.conf

ipvar HOME_NET any > ipvar HOME_NET192.168.1.0/24

Následující změny v konfiguračním souboru upřesňují cesty k pravidlům

var RULE_PATH ../rules

var SO_RULE_PATH ../so_rules

var PREPROC_RULE_PATH ../preproc_rules

var WHITE_LIST_PATH ../rules

var BLACK_LIST_PATH ../rules

Změnit na:

var RULE_PATH /etc/snort/rules

var SO_RULE_PATH /etc/snort/so_rules

var PREPROC_RULE_PATH /etc/snort/preproc_rules

var WHITE_LIST_PATH /etc/snort/rules/iplists

var BLACK_LIST_PATH /etc/snort/rules/iplists

Přidať řádek 545

include $RULE_PATH/snort.rules

#include $RULE_PATH/local.rules

Barnyard 2 slouží na komunikaci binárních souborů

vi /etc/snort/snort.conf

Řádek: 521

output unified2: filename merged.log, limit 128, nostamp, mpls_event_types,

vlan_event_types

změniť na:

output unified2: filename snort.u2, limit 128

Konfigurace Barnyard2

vi /etc/snort/barnyard2.conf

Na konec souboru je potřeba napsat odkaz na databázi:

output database: log, mysql, user=snort password=123456 dbname=snort host=localhost

chmod o-r /etc/snort/barnyard2.conf

Pulledpork slouží na automatické stahování a aktualizaci pravidel. Na dvou místech je třeba napsat oinkcode, který dostanete po registraci na oficiální stránce Snort:

61a13c1fea16adbdb7489b948d630f405e3a6352

vi /etc/snort/pulledpork.conf

Odkomentovat:

rule_url=https://rules.emergingthreats.net/|emerging.rules.tar.gz|open-nogpl

Řádek 74:

rule_path=/usr/local/etc/snort/rules/snort.rules
změnit na:
rule_path=/etc/snort/rules/snort.rules
Řádek 89:
local_rules=/usr/local/etc/snort/rules/local.rules
změnit na:
local_rules=/etc/snort/rules/local.rules
Řádek 92:
sid_msg=/usr/local/etc/snort/sid-msg.map
změnit na:
sid_msg=/etc/snort/sid-msg.map
Řádek 96:
sid_msg_version=1
změnit na:
sid_msg_version=2
Řádek 119:
config_path=/usr/local/etc/snort/snort.conf
změnit na:
config_path=/etc/snort/snort.conf
Řádek 133:
distro=FreeBSD-8.1
změnit na:
distro=Ubuntu-12-04
Řádek 141:
black_list=/usr/local/etc/snort/rules/iplists/default.blacklist
změnit na:
black_list=/etc/snort/rules/iplists/black_list.rules
Řádek 150:
IPRVersion=/usr/local/etc/snort/rules/iplists
změnit na:
IPRVersion=/etc/snort/rules/iplists

Aktualizace pravidel Snort:
/usr/local/bin/pulledpork.pl -c /etc/snort/pulledpork.conf –l

Spuštění systému Suricata:

suricata -c /etc/suricata/suricata.yaml -i eth1 –init-errors-fatal

Výstrahy se ukládají do souboru fast. log, zobrazíte si ho pomocí příkazu cat /var/log/suricata/fast.log

Spuštění systému Snort:
/usr/local/bin/snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i eth1

Výstrahy se budou zobrazovat automaticky.

Před zahájením útoku počkejte dvě minuty.

3. Pomocí různých druhů útoků testujte nastavení systémů.

SYN flood	hping3 -c 100000 -d 120 -S –flood 192.168.1.x
UDP flood	hping3 -2 –flood 192.168.1.x
HTTP flood	hping3 -c 100000 -d 50 -p 80 –flood 192.168.1.x
Ping of Death	hping3 -c 100000 -d 500 -p 20 -1 –flood 192.168.1.x
RAW IP paket	hping3 -c 100000 -d 8 -0 –flood 192.168.1.x

Samostatná práce:

- Zamyslete se, jak je potřeba nastavit pravidla pro správné fungování.
- Jak by mělo vypadat grafické rozhraní pro IDS/IPS systémy.
- Napište nové pravidlo v systému Suricata a otestujte ho útokem.

B OBSAH PRILOŽENÉHO USB

Priložený USB kľúč obsahuje elektronickú verziu bakalárskej práce a laboratórnej úlohy vo formáte PDF. 4 virtuálne stroje s počiatočnou konfiguráciou, ktoré sa implementujú do OS VirtualBox. Videonahrávky s vypracovaním laboratórnej úlohy.