Jihočeská univerzita v Českých Budějovicích

Přírodovědecká fakulta

Detekce a analýza průniků systémy IDS a IPS

Bakalářská práce

David Szep

Vedoucí práce: Ing. Rudolf Vohnout

Školitel: Ing. Petr Břehovský

České Budějovice 2013

Bibliografické údaje

Szep D., 2013: Detekce a analýza průniků systémy IDS a IPS.

[Intrusion detection and analysis of IDS and IPS. Bc. Thesis, in Czech.] – 52 p., Faculty of Science, University of South Bohemia, České Budějovice, Czech Republic.

Abstrakt

Tato bakalářská práce se zabývá bezpečnostními systémy IDS a IPS, které jsou realizovány nástrojem Snort. V teoretické části je vysvětlena problematika zabezpečení síťové infrastruktury, zejména využitím IDS/IPS. V praktické části je testována schopnost bezpečnostního systému detekovat vybrané počítačové útoky. Výsledkem práce jsou popsané hrozby, které Snort zachycuje a naopak, které není schopný detekovat. Závěrem je navrženo optimální nasazení bezpečnostního systému v síti.

Abstract

This thesis deals with security systems IDS and IPS which are implemented by Snort tool. The theoretical part explains the issue of the network security infrastructure, mainly using IDS/IPS. The practical part dwells on the testing of the ability of the security system to detect selected cyber attacks. The results of the work describe threats that Snort is able and unable to detect and to capture. Finally, the optimal deployment of the security system in the network is proposed.

Klíčová slova

firewall, IDS, IPS, Snort, pravidlo, výstraha, útok, útočník, DoS, Hping, SQL injection, Burp, skenování, Nmap, šifrování, OpenSSL, OpenVPN, optimální nasazení

Key words

firewall, IDS, IPS, IDPS, Snort, rule, warning, attack, attacker, DoS, Hping, SQL injection, Burp, scanning, Nmap, encrypted, OpenSSL, OpenVPN, optimal deployment

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Českých Budějovicích, dne 13. 12. 2013.

Podpis: .....

Poděkování

Rád bych poděkoval v první řadě Ing. Petru Břehovskému za všechny cenné rady a obzvláště pomoc při realizaci počítačových útoků, dále Ing. Rudolfu Vohnoutovi za odborné vedení práce a pomoc při zpracování a také slečně Bc. Tereze Smejkalové za pomoc se slohovou stránkou práce. Na závěr také přátelům a rodině za podporu.

Obsah

ÚVOD **1**

1 MONITORING SÍTĚ **3**

2 FIREWALL **4**

2.1 TYPY FIREWALLU 5
2.2 CO FIREWALL ZARUČÍ 5
2.3 CO FIREWALL ZARUČIT NEMŮŽE 6
2.4 FIREWALLY NOVÉ GENERACE 6

3 BEZPEČNOSTNÍ SYSTÉMY IDS/IPS **7**

3.1 SYSTÉM IDS (INTRUSION DETECTION SYSTEM) 8
3.2 SYSTÉM IPS (INTRUSION PREVENTION SYSTEM) 8
3.3 DETEKČNÍ METODY 8
3.4 ROZDĚLENÍ PODLE UMÍSTĚNÍ (TOPOLOGIE) 9
3.5 SPECIÁLNÍ ROZŠÍŘENÍ 10
3.6 SHRNUTÍ 11

4 SNORT **12**

4.1 REŽIMY SYSTÉMU SNORT 12
4.2 PRAVIDLA SNORTU 14
4.3 FORMÁT VÝSTRAHY 16
4.4 SHRNUTÍ 16

5 POČÍTAČOVÝ ÚTOK OBECNĚ **17**

5.1 POČÍTAČOVÝ ÚTOČNÍK 17
5.2 DŮVODY POČÍTAČOVÝCH ÚTOKŮ 17
5.3 OBECNÝ POSTUP ÚTOKU 18

6 VYBRANÉ POČÍTAČOVÉ ÚTOKY **19**

6.1 SQL INJECTION 19
6.2 DOS (DENIAL OF SERVICE) 20
6.3 DDOS 22
6.4 ZAŠIFROVANÝ PŘENOS 23

7 SESTAVENÍ SÍTĚ **24**

7.1 SCHÉMA ZAPOJENÍ 24
7.2 POSTUP TESTOVÁNÍ 25

8 TESTOVÁNÍ 28
8.1 SKENOVÁNÍ CÍLE 28
8.2 SYN FLOOD ATTACK 31
8.3 SQL INJECTION 32
8.4 ŠIFROVANÝ PŘENOS INFORMACÍ 34
8.5 ZAŠIFROVANÝ TUNEL 36
8.6 PŘEHLED TESTOVÁNÍ 37
9 IMPLEMENTACE IPS 37
10 OPTIMÁLNÍ NASAZENÍ IDS/IPS 38
10.1 UMÍSTĚNÍ V SÍTI 38
10.2 VOLBA SYSTÉMU 39
10.3 NÁVRH OPTIMÁLNÍHO NASAZENÍ BEZPEČNOSTNÍHO SYSTÉMU 40
ZÁVĚR 41
SEZNAM LITERATURY 43
SEZNAM OBRÁZKŮ 45
PŘÍLOHA 1 46
PŘÍLOHA 2 49
PŘÍLOHA 3 50
PŘÍLOHA 4 51
PŘÍLOHA 5 52
PŘÍLOHY 52

Úvod

Tato bakalářská práce se věnuje bezpečnosti síťové infrastruktury, zejména prostřednictvím bezpečnostního systému IDS/IPS. Téma bylo zvoleno především kvůli vlastnímu zájmu o tuto problematiku a z důvodu rozšíření vlastních znalostí v oboru, kterému bych se i nadále rád věnoval.

V případě, že by práci studoval čtenář, který není v oboru příliš zdatný, je po celý průběh práce kladen důraz výstižně publikovat teoretická fakta s následnou praktickou ukázkou a vysvětlením. V praktické části je kladen důraz především na ukázky společně s použitou metodikou.

Samotná práce obsahuje obecný úvod do problematiky bezpečnosti, kdy je potřeba zdůraznit, jak důležité je sledování aktivit na síti a bránit se útokům pomocí bezpečnostních nástrojů dnešní doby. Kromě firewallu, který musí být nezbytnou součástí zabezpečení sítě, se práce věnuje především kompletnímu nasazení IDS/IPS v síti. Tento bezpečnostní systém je realizován nástrojem Snort, který analyzuje síťový provoz, případně reaguje na nebezpečné podněty. Po přečtení teoretické části by čtenář měl získat informace o tom, jak daný nástroj pracuje, z jakých se skládá komponent, jaké generuje výstupy (výstrahy), případně o co by mohl být ještě rozšířený. Dále je předložen teoretický základ bezpečnostních hrozeb, které jsou v práci využity, a také pojednání o obraně, kterou je možné aplikovat k zajištění maximálního zabezpečení.

Po seznámení čtenáře s obecnou problematikou bezpečnosti a systémem IDS/IPS, je sestavena topologie sítě, která vystihuje reálnou strukturu sítě menší společnosti. V této síti jsou realizovány počítačové útoky ve snaze otestovat detekční schopnost IDS/IPS a dosáhnout hlavního cíle práce, kterým je přechytračit bezpečnostní systém. Celý průběh testování probíhá v laboratorních podmínkách, kde není veden běžný provoz sítě, tudíž se bezpečnostní systém může plně věnovat detekci simulačních útoků a tím je testování systému optimální a získané výsledky zcela nezkreslené. Použité útoky jsou vybrány ve snaze pokrýt nejaktuálnější počítačové hrozby jak z vnější sítě, tak z vnitřní sítě a zároveň takové, které mohou být schopny obejít bezpečnostní systém. Před provedením každého útoku je nutné získat informace o cílovém hostiteli. Nmap je jedním z nejpoužívanějších nástrojů právě pro získání těchto informací, a tak je testována

schopnost bezpečnostního systému reagovat na pakety odeslané právě nástrojem Nmap. Útok z vnější sítě je realizován prostřednictvím útoku zvaného DoS, konkrétně SYN flood attack. Útok z vnitřní sítě realizován pomocí SQL injection. Další postup experimentování testuje detekční schopnost IDS/IPS vůči zašifrované komunikaci, což je věc v síťové komunikaci stále častěji využívaná. Provedené experimenty přináší zajímavé výsledky a způsoby přechytračení bezpečnostního systému. Pro přehlednost je vytvořena tabulka, která obsahuje souhrn získaných výsledků.

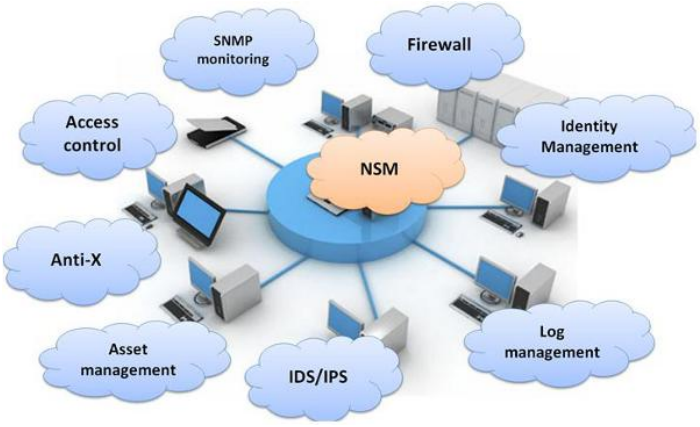
Vedlejší cíl bakalářské práce je optimální nasazení IDS/IPS v síti, čemuž se věnuje druhá polovina praktické části. Za základě experimentování a získaných zkušeností je navržen způsob, jak lze bezpečnostní systém umístit v síti, aby byla zajištěna maximální bezpečnost. Dále také pojednání o tom, jaký způsob implementace systému zvolit. V práci jsou navrženy dva způsoby, z nichž každý má své klady i zápory. Především se jedná o poměr mezi cenou a zajištěnou bezpečností.

I. Teoretická část

1 Monitoring sítě

S přibývajícími technickými vymoženostmi, které mají pomoci zlepšit životní situaci každého z nás, jsou tu i tací, kteří se snaží tyto vymoženosti zneužít ve svůj prospěch. Typickým příkladem je zneužití dat skrz internetovou síť. Obdobné myšlení většiny je takové, že k internetu jsou připojeny miliony lidí, proč by se něco mělo stát zrovna mně? Když se ale útočník nebo škodlivý kód dostane do vnitřní sítě, už bývá pozdě a útočník získává cenný lup, především v podobě citlivých dat. Aby bylo těmto nepříjemnostem zabráněno, je dobré si uvědomit jednu zásadní věc: Monitoring sítě je nezbytný!

Obecně lze mluvit o dvou typech sledování sítě, a to o periodickém a nárazovém. [1] V obou případech se uvnitř sítě nachází sledovací zařízení (o kterých se více budou zmiňovat další kapitoly), které sleduje aktuální provoz sítě. Při periodickém sledování systém zapisuje informace v reálném čase nebo jej vypisuje přímo na obrazovku. U nárazového sledování se většinou jedná o reakci na určité podněty, změny apod. Monitorovat lze téměř každou činnost v systému od elektronické pošty přes přihlašovací pokusy až po detekci škodlivého kódu. [1]



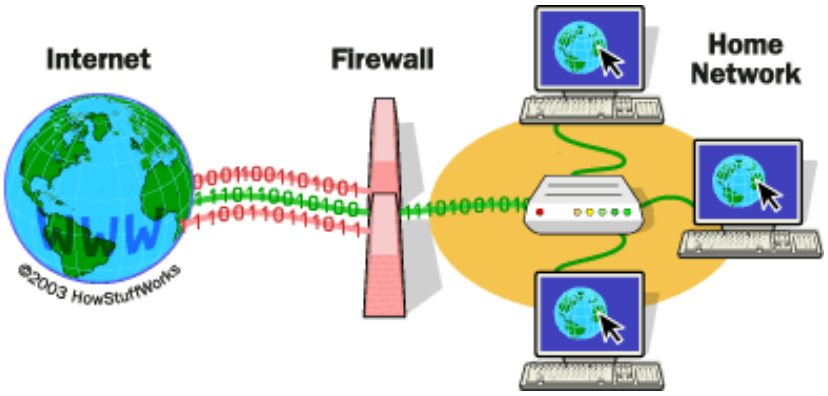
Obrázek 1 - Bezpečnostní struktura vnitřní sítě[1]

[1] Zdroj: http://www.ictsecurity.cz/images/10/advad0725.png

Pro správné sledování musí správce sítě zvolit optimální nástroje. Měl by zvážit, jak citlivá data by mohl případný útočník získat a tomu přizpůsobit míru zabezpečení. Dále zvážit především částku, kterou do zabezpečení společnost investuje nebo jakou bezpečností politiku zvolí.

2 Firewall

Monitoring sítě a bezpečnost uživatele na internetu je velmi důležitým aspektem. Firewall je bezpodmínečně základním kamenem bezpečnosti před útoky zvenčí. Jako výstižný příklad může být uveden vodní příkop kolem středověkého hradu. Vstupní i výstupní místo vede skrz kontrolní pásmo (bránu). Při průchodu skrz firewall se datový tok analyzuje a vyhodnocuje. Záleží na nastavení správce bezpečnosti, zda daný tok zakáže, povolí nebo omezí (například pokud uživatelům za firewallem umožní navštěvovat určitou stránku). Na první pohled se může zdát, že zabezpečení je dokonalé, ale stejně tak, jako hrady s vodními příkopy byly dobity, ani firewall nezajišťuje kompletní ochranu.



Obrázek 2 - Firewall[2]

[2] Zdroj: http://static.ddmcdn.com/gif/firewall.gif

2.1 Typy firewallu

2.1.1 Paketové firewally

Jelikož paketové firewally pracují na principu kontroly zdrojové, cílové IP adresy a zdrojového, cílového portu (třetí a čtvrtá vrstva OSI modelu), jejich zabezpečení nedosahuje příliš vysoké úrovně. Další nevýhoda leží ve správě a administraci. Neposkytují ukládání do logu, ani nehlásí případnou detekci. Naopak velice malá operativní náročnost těchto firewallů zaručuje velmi vysokou rychlost. Používají se zejména na routerech, kde se uplatní především díky své vysokorychlostní operační dovednosti. [3]

2.1.2 Aplikační firewally

Aplikační firewally pracují na sedmé (aplikační) vrstvě síťového OSI modelu. Předností je především analýza příloh elektronické pošty nebo kontrola FTP spojení. Použitím tohoto firewallu doslova dojde k oddělení vnitřní sítě od vnějšího internetového světa. Při komunikaci do vnitřní sítě je navázáno spojení s firewallem a poté firewall inicializuje spojení s vnitřní sítí (obdobně pracuje i spojení opačným směrem). Z praktického hlediska se jedná o mnohem bezpečnější vnitřní síť než v případě paketového typu firewallů, ale velkou nevýhodou je hardwarová náročnost. [3]

2.1.3 Stavový firewall

Princip stavového firewallu je založený na kontrole obdobně jako paketové typy s rozdílem, že stavové firewally evidují již navázané spojení, čímž nemusí znovu procházet bezpečnostním schvalováním a tím se stávají daleko efektivnějšími, rychlejšími a také úroveň bezpečnosti je na velice vysoké úrovni. Dá se tedy říci, že stavový firewall spojil kladné vlastnosti předchozích firewallů, což je rychlost, efektivita a bezpečnost.[4]

2.2 Co firewall zaručí

Bez ohledu na to jaký typ firewallu je používán, lze metaforicky říci, že firewall je policistou, který pracuje na bázi pravidel. Má stanovena předem konfigurovaná pravidla, podle kterých se komunikace řídí. Pokud se tato pravidla poruší, komunikace je zakázána. [2]

2.3 Co firewall zaručit nemůže

Firewall dokáže kontrolovat komunikaci do sítě i ze sítě, ale pokud nastane případ, kdy je útočník již ve vnitřní síti (uživatel vnitřní sítě), nic mu pak nebrání jakákoliv data zkopírovat a vynést z vnitřní sítě. [2]

Podstatné rovněž je, že firewall je předem nakonfigurován a je účinný pouze na "známou hrozbu". V případě, kdy se objeví nová hrozba, nemá nejmenší tušení o tom, že propouští do vnitřní sítě škodlivý kód. [2]

2.4 Firewally nové generace

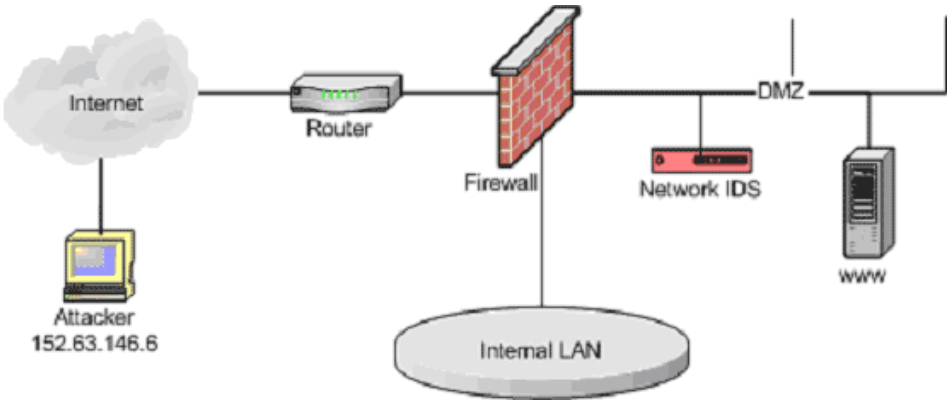
Firewall je sice základem bezpečné sítě, ale jsou věci, na které jsou jeho funkce krátké. Vychytralost dnešních hackerů dosáhla takové úrovně, že běžně používané firewally (většinou stavové) mají primárně otevřený port 80 (http) a nedokážou rozpoznat, jakým aplikacím nabízí danou službu a zdali jde o nelegální přístup. Z toho hlediska se začalo pracovat na firewallech tzv. nové generace (NGFW). [5]

Tyto firewally spojují služby firewallu, IDS/IPS a dalších bezpečnostních systémů do jednoho vysoce účinného nástroje. Tímto krokem dochází jednak ke zvýšení zabezpečení a také ke snížení celkových nákladů. Obvykle bylo v síti více zařízení za sebou, aby pokryly veškeré hrozby, což s NGFW neplatí. [5] Z pohledu zabezpečení spočívá velká výhoda NGFW v tom, že filtrování a detekce hrozeb je daleko účinnější než v kombinaci různých externích zařízení. Jednoduchým příkladem může být použití programu Skype. Zatímco firewall zjistí, o jakou službu se jedná, systém IDS/IPS se již může zaměřit na známé hrozby právě přes tuto službu. [5]

S nástupem NGFW je sice bezpečnost sítě na vysoké úrovni, problém však spočívá ve výkonu. Otázka zní, zdali je tento systém schopný rozšifrovat data (SSL), provést potřebnou analýzu, komunikaci opět zašifrovat a poslat dál. I když bude předpoklad takový, že toto systém zvládne, musí se vzít v úvahu, s jakým vlivem na výkon. [5] Podle NSS Labs při spuštění integrovaného systému IDS/IPS sníží se výkon celkového systému o 60 procent (z 10Gb/s na 4Gb/s). Pokud bychom použili i vnitřní integrovaný antivirový systém, výkon by poklesl na 300Mb/s až 400Mb/s. V neposlední řadě také nastavení pravidel a jejich složitost hraje ve výkonu zásadní roli.

3 Bezpečnostní systémy IDS/IPS

Obecně lze říci, že na těchto systémech je v dnešní době postavena bezpečnostní politika organizací, které potřebují chránit svojí síť před hrozbami na maximální úrovni. Tyto systémy kontrolují datový tok a v případě odhalení abnormálního jevu reagují (pasivně, aktivně). Většinou se jedná o spojení hardwaru a softwaru, ale mohou být pouze softwarové produkty této ochrany, které jsou zpravidla realizovány vlastním operačním systémem.



Obrázek 3 - Umístění IDS v síti[3]

Skutečnost je ale taková, že i když máme plně aktualizovaný software a zapnutý firewall, může být naše síť napadena. I přes veškeré toto zabezpečení útočník zašle škodlivý kód na e-mail nebo přes dnes velmi oblíbenou sociální síť facebook, což znamená, že bezpečně projde skrze zabezpečení jako běžná zpráva. Poté uživatel otevře tuto zprávu a tím vlastně také zadní vrátka do svého systému. [6]

Ani aplikací IDS by se moc nezměnilo, jelikož nedokáže aktivně reagovat. O něco užitečnější by se mohlo zdát použití aktivní ochrany IPS, ale je zde plno vedlejších faktorů, které je potřeba zhodnotit. Příkladem může být zamezení legitimní komunikace a následkem toho může společnosti přijít o zisk z prodeje. Následující kapitoly se této problematice budou věnovat detailněji.

[3] Zdroj: https://www.sans.org/resources/idfaq/role1.gif

3.1 Systém IDS (Intrusion Detection System)

Systém monitoruje síťový provoz a upozorňuje na potenciálně nebezpečnou komunikaci, která je vyhodnocována podle předem konfigurovaných pravidel. Právě proto, že "pouze" vydává upozornění a nezasahuje do procházející komunikace, je tento bezpečnostní systém označován jako pasivní.

Částečnou aktivitou může být konfigurování IDS, aby aktivně spolupracoval s firewallem. Touto spoluprací je myšleno zaslání TRAP příkazu bezpečnostním systémem na firewall, kde je generováno pravidlo, které zakáže průchod nežádoucího spojení. Další možností jak zabránit útočníkovi v průniku do sítě je zaslání "TCP reset", v případě protokolu UDP, "ICMP unreachable port". [7] Ve všech případech je sice zastavena potencionálně nebezpečná komunikace, ale spojení už bylo navázáno a nemůžeme tedy hovořit o aktivní ochraně.

3.2 Systém IPS (Intrusion Prevention System)

O tomto systému je hovořeno jako o rozšíření IDS. Tento systém nejenže detekuje neobvyklé aktivity, zaznamenává a upozorňuje stejně jako IDS, ale jeho velkou předností je také aktivní ochrana sítě, tzn. okamžitá reakce na incidenty. V případě detekce nežádoucí aktivity systém zablokuje daný provoz nebo je schopný kompletně zamezit spojení ze zdrojové IP adresy. V případě IDS, který čeká na vyhodnocení správcem bezpečnosti, IPS jedná samostatně. [7] Problém nastává tehdy, pokud se jedná o tzv. planý poplach. Tam, kde správce sítě by vyhodnotil danou hrozbu jako negativní, systém IPS reaguje a může způsobit značné škody. V případě IPS musí být konfigurace bezpečnostního systému velice citlivá, aby bylo vyhodnoceno co nejméně planých poplachů a zároveň bezpečnost zůstala na co nejvyšší úrovni.

3.3 Detekční metody

Následuje výčet detekčních metod, které systém IDS/IPS využívá k odhalení nežádoucí komunikace.

3.3.1 Detekce podle vzoru

Princip této metody spočívá v hledání známých evidovaných vzorů škodlivého kódu (tzv. signatur). Systém analyzuje procházející pakety a hledá v nich shodu právě s

nebezpečnými vzory. Pokud by škodlivý kód byl rozdělen do více paketů, je schopný pakety rekonstruovat. [7]

3.3.2 Detekce odchylek

Vychází se standardu RFC 4380 (definice jednotlivých protokolů). Pokud probíhající síťový provoz neodpovídá standardní komunikaci, je tato odchylka detekována a dále analyzována. [7]

3.3.3 Detekce anomálií

Síťový provoz je porovnáván na základě statistických metod. Pokud se vymyká běžnému provozu, je vydána výstraha a neznámá komunikace se hlouběji analyzuje. [7]

3.3.4 Shrnutí

Metoda detekce vzoru je velmi přesná a spolehlivá, ale omezená pouze na detekci již známých popsaných signatur. Nepopsané a neevidované útoky není schopna detekovat. Oproti tomu metoda detekce anomálií nebývá sice tak spolehlivá (riziko velkého množství falešných poplachů), ale dokáže upozornit i na zatím neznámé a neevidované útoky. Praxe většinou bývá taková, že se metody kombinují a tudíž navzájem doplňují.

3.4 Rozdělení podle umístění (topologie)

Podle umístění detekčních systémů v síti lze rozdělit IDS/IPS na Host-based a Network-based. Liší se především tím, kde jsou v síti umístěny a jakou funkci vykonávají.

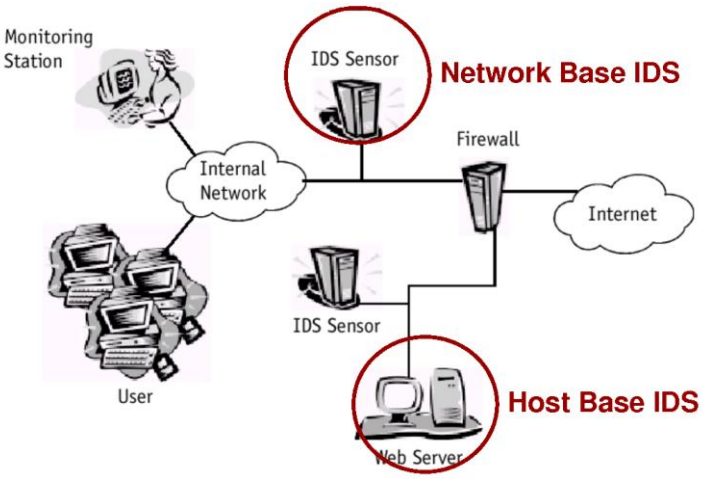
3.4.1 Host-based IDS/IPS

Jejich umístění je především na uživatelské stanici nebo na serverovém PC. Jelikož se ve většině případů jedná o SW provedení, jsou závislé na tom, jaký operační systém je na konkrétním PC používán. Úkolem Host-based systémů je kontrola veškeré komunikace právě na této stanici, zaznamenávání aktivit a případně vydání výstrahy na potencionálně nebezpečné podněty. [7] Jak už bylo zmíněno, Host-based systém je závislý na operačním systému konkrétní stanice, což je velkou nevýhodou. Na každý operační systém se provádí jiná konfigurace, z čehož vyplývá vysoká znalostní náročnost na správce bezpečnosti.

3.4.2 Network-based IDS/IPS

Na rozdíl od předchozího typu není umístěn na konkrétní stanici, ale pokud možno na nejfrekventovanějším místě v dané síti a kontroluje datový provoz skrz celou vnitřní síť. Obvykle je tato kontrola prováděna na tzv. síťovém vstupu, kde prochází veškerý síťový provoz a je možné jej analyzovat. Důležité je, aby bezpečnostní systém monitoroval běh a zároveň neovlivňoval chod celé sítě, což je v určitých případech problém. Jako každý systém je i tento omezen určitou rychlostí a kapacitou, v čemž spočívá obrovská nevýhoda. Pokud bude síť zahlcena velkým množstvím dotazů, systém nebude schopen kontroly všech paketů, což může být hrozbou pro vnitřní síť. [8]

Závěrem je potřeba zmínit, že kombinací HIDS a NIDS lze dosáhnout vysokého stupně zabezpečení. Musí se však brát v potaz velice obtížná implementace, konfigurace systémů a v neposlední řadě správa celé sítě.



Obrázek 4 - Host-based vs. Network-based[4]

3.5 Speciální rozšíření

Vybavení některých IDS/IPS systémů není zcela obvyklé. Obsahují speciální rozšíření, které umožňuje efektivnější detekování nebo tzv. samokonfiguraci. Většinou jsou tato rozšíření aplikována přímo výrobci, při vlastní konfiguraci podobných rozšíření by konfigurace byla velmi náročná. Nutné je dodat, že se obvykle jedná o komerční, zpravidla velice nákladné, nástroje.

[4] Zdroj: http://img.docstoccdn.com/thumb/orig/99491910.png

3.5.1 Skenovací nástroj

Skenovací nástroj je schopen zajistit automatickou konfiguraci bezpečnostního systému. Ihned po zavedení do sítě analyzuje uživatelské stanice, operační systémy a aplikace zde provozované. Po této analýze se na základě výsledků přizpůsobí dané síti. [7]

3.5.2 Honeypot

Dalším zajímavým rozšířením, které lze na systému IDS/IPS aplikovat, je Honeypot. Jedná se o virtuální počítač, který má svojí vlastní IP adresu a je z pohledu útočníka lehkou kořistí. V případě útoku na Honeypot je útočník okamžitě odhalen.[7]

3.5.3 WIPS (Wireless Intrusion Prevention System)

Při pohledu do budoucna, je stále více kladen důraz na mobilitu uživatelů, s čímž samozřejmě souvisí bezdrátový přenos dat. I takový přenos je potřeba chránit před nežádoucí komunikací. K tomuto účelu byly vyvinuty tzv. WIPS (Wireless Intrusion Prevention System). Jejich úkolem je především kontrolovat rádiovou komunikaci přístupových bodů. V praxi to znamená, že senzory přepínají mezi přenosem dat a vyhledáváním případné detekce. Tento sdílený postup se nazývá časové vzorkování (time slicing). Aby vliv na klienta a na celkový výkon sítě nebyl značný, časové vzorkování probíhá ve velmi krátkých časových intervalech. Pro představu vyjádřením v čase, méně než jednu vteřinu každou minutu, což znamená, že každý den je provoz 23 hodin a 36 minut nechráněný. Systém WIPS je tedy schopný zachytit pouze zjevné a časově náročnější úkony. [8]

3.6 Shrnutí

Bezpečností systém IDS/IPS je velmi efektivním nástrojem pro zabezpečení síťového provozu, zpravidla výborným rozšířením základního firewallu. Velkým rozdílem mezi systémy IDS a IPS je reakční doba na incident, v obou případech je však upozorněn správce sítě. Pro zvýšení účinnosti daných metod zabezpečení je potřeba pravidelné aktualizace znalostní databáze signatur. Reakční doba bezpečnostních společností na nové hrozby je obvykle v řádu hodin. Výhodou je možnost psaní vlastních pravidel a signatur, podle kterých se systémy řídí. [7] Skutečnost je taková, že po implementaci tohoto druhu bezpečnostního systému je potřeba několikatýdenního testování a případného dolaďování.

4 Snort

V dnešní době je Snort jedním z nejrozšířenějších detekčně/prevenčních systémů. Jeho široké rozšíření je zapříčiněno zejména tím, že se jedná o open-source nástroj, což znamená volně šiřitelný software. Snort nemá nouzi o pravidelný vývoj, aktualizování a vylepšování. Velkou výhodou je implementace napříč operačními systémy (Windows, Unix, Mac OS atd.). Dále také možnost vlastní konfigurace systému, především psaní vlastních pravidel, díky čemuž má uživatel možnost redukovat falešné poplachy nebo se zaměřit na určitý druh napadení. Obzvláště falešné poplachy jsou velmi nežádoucí aktivitou a vlastní vhodnou konfigurací jim lze předcházet. [12] Je nutné si uvědomit, že nelze systém nakonfigurovat tak, aby nedocházelo k žádným falešným poplachům a zároveň byla síť stoprocentně chráněna. Vždy je nutné zvolit nejoptimálnější konfiguraci.

4.1 Režimy systému Snort

Starší verze systémů pracovaly pouze v režimu paket sniffer. [12] Už ale byla řeč o vývoji a vylepšování – a to je příčina toho, že se systém rozšířil o další dva režimy, paket logger a network intrusion detection system (NIDS).

4.1.1 Paket sniffer

Paket sniffer, česky označovaný jako štěnice, slídič nebo také čichač. Princip tohoto režimu je v tom, že zachytává procházející pakety a vypisuje je přímo na obrazovku.

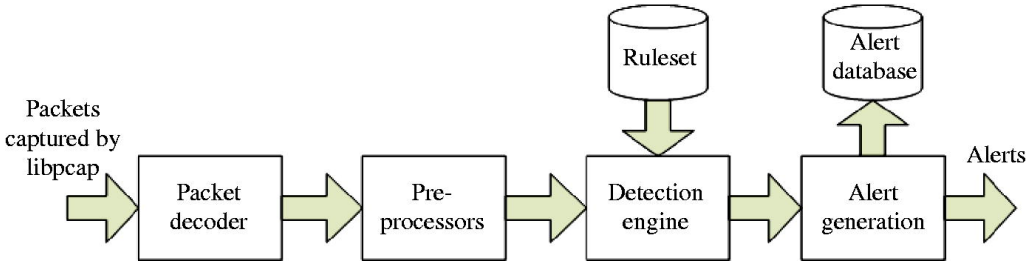
4.1.2 Paket logger

Paket logger, česky označovaný jako záznamník. Pracuje na podobném principu jako paket sniffer s tím rozdílem, že tento režim navíc zaznamenává data na disk.

Tyto dva režimy provádějí v principu stejné operace – zachytávání síťového provozu a následné zpracování paketů, ať už na disk do souboru nebo v obrazové podobě na monitoru. Obdobné operace provádí software jako je wireshark (příjemné uživatelské rozhraní) nebo tcpdump (v základní Linuxové výbavě), proto se tyto dva režimy obvykle přes Snort neprovádějí. Daleko praktičtější a nejvíce užívaný režim Snortu je NIDS (Network Intrusion Detection System).

4.1.3 NIDS

V tomto režimu Snort nezaznamenává veškeré pakety, ale pracuje na principu analýzy a vyhodnocení podle předem definovaných pravidel. Snort v režimu NIDS vyhodnocuje, které pakety budou analyzovány. Tím se výrazně zvyšuje výkon Snortu a snižuje se pravděpodobnost falešných poplachů. Snort obsahuje několik zásuvných modulů (komponent), kterými pakety procházejí. [12]



Obrázek 5 - Snort komponenty[5]

Celý síťový provoz prochází skrz zásuvné modely preprocesoru, které rozhodují o tom, které pakety budou dále analyzovány. K takovému rozhodování slouží tzv. packet classifier, který zkoumá dané pakety a rozhoduje, zda je paket například token ring nebo ethernetový rámec, o jaký typ protokolu se jedná (TCP,UDP apod.), jestli se jedná o IP nebo non-IP rámec, zda je rámec součástí VLAN atd. [12] Pokud je paket vyhodnocen jako potenciálně nebezpečný, je skenován detekční jednotkou.

Detekční jednotka porovnává dané pakety podle předem konfigurovaných pravidel, například hledání určitých klíčových slov, hledání určitého obsahu (binární řetězec realizující útok) nebo hledání anomálií (specifická hlavička nebo vlastnosti paketu - ICMP pakety delší než 800 bytů). Tato analýza se provádí na úrovni síťové vrstvy OSI modelu.

Součástí detekční jednotky je i tzv. IP defragmenter, který rozděluje IP datagram do dvou nebo více menších částí a poté jej opět skládá dohromady. Důvodem je, že IP datagramy mohou přicházet v různém pořadí nebo třeba i různými cestami. Cílem IP defragmenteru je tedy ukládat datagramy ve vyrovnávací paměti podle cíle a až poté různé fragmenty datagramu skládat dohromady. Opravdu kvalitně navržené IDS/IPS

[5] Zdroj: http://opentodo.files.wordpress.com/2012/10/snort-architecture.png

dokážou odhalit i souvislosti datagramů odeslané z různých operačních systémů (datagram různých operačních systémů má odlišnou strukturu). V případě, že bezpečnostní systém není dobře navržen, je to způsob, kterým lze IDS/IPS úspěšně obejít. [12]

Pokud je IP datagram na síťové vrstvě zpět zkonstruován, Snort pokračuje zkoumáním na transportní vrstvě, tzv. segmentu. Toto zkoumání zajišťuje modul zvaný stream5. Šetření na transportní vrstvě probíhá obdobně jako na síťové vrstvě. [12]

Další vrstvou, kde je síťový provoz kontrolován, je relační vrstva. Útočník, než se rozhodne útok uskutečnit, musí nejdříve detailně analyzovat svůj cíl. Toto zkoumání cílového hostitele probíhá právě na relační vrstvě OSI modelu. Jedná se zejména o zjištění, na jakém systému cílová služba běží, pod jakým typem protokolů, případně jaké porty jsou dostupné. K získání těchto informací je velice užitečný program Nmap. Další vlastností programu Nmap, kromě skenování svého cíle, je například zfalšování zdrojové IP adresy. K detekci právě takovýchto aktivit obsahuje Snort preprocesor zvaný sfportscan. [12]

Po provedení výše zmíněných šetření a v případě detekování nežádoucí aktivity jsou generovány výstrahy (Snort využívá SNMP protokol - Simple Network Management Protocol) a zpravidla provedeno logování výstrah (do souboru, databáze).

4.2 Pravidla Snortu

Samovolná konfigurace a editování pravidel je jednou z nejužitečnější vlastností, kterou lze na Snortu ocenit.

Pravidla Snortu využívají specifikovaný konfigurační jazyk, který je jednoduchý a velmi flexibilní. Jako každý jazyk má i tento své zásady. Například v dřívějších verzích bylo nutné psát pravidla v jediném řádku, to se od verze 1.8 mění a je možno řádkovat za použití zpětného lomítka. [14]

Snort pravidla lze rozdělit na dvě části - hlavička a tělo.

Obecný předpis hlavičky:

- *akce protokol zdroj_ip zdroj_port -> cíl_ip cíl_port (tělo)*

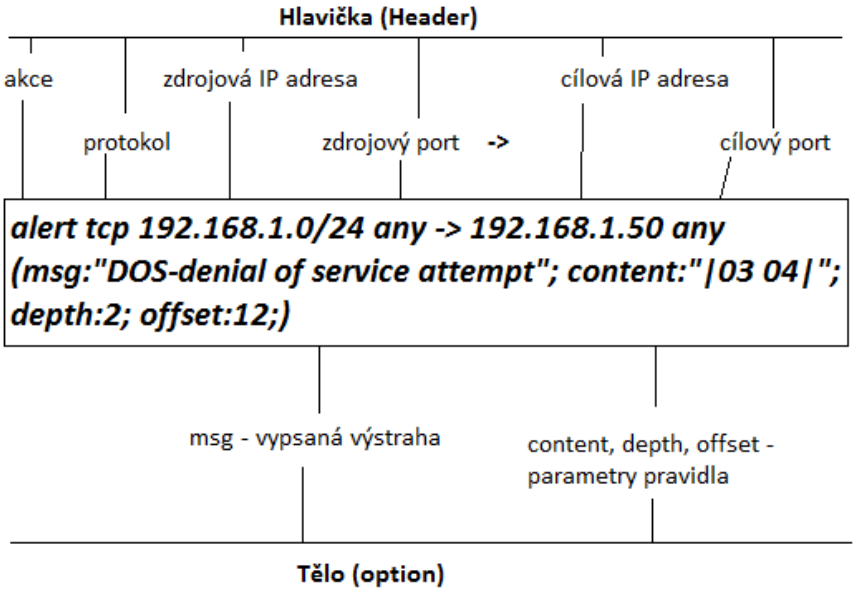
Hlavička obsahuje typ protokolu (TCP,UDP atd.), zdrojovou a cílovou IP adresu (včetně masky), zdrojový a cílový port a také akce, která bude s paketem provedena.

- alert – upozornění
- log – záznam
- pass – ignorace paketu
- aktiv – aktivní ochrana
- drop – blokace a zalogování
- reject – blokace, zalogování a přerušení spojení

Lze využít i logických operátorů, například rozsah IP adres nebo portů. [14]

Tělo pravidla obsahuje nastavení, kritéria, zprávy, informace aj. podle kterých je paket kontrolován. Při použití více možností se od sebe oddělují pomocí středníku.

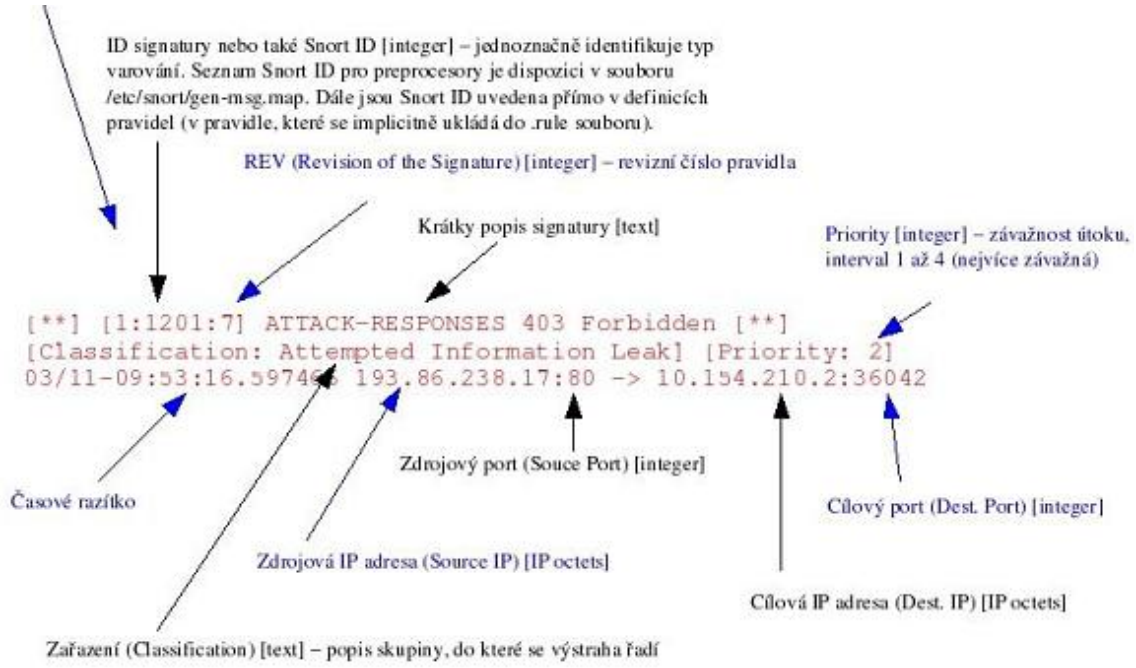
Tento jednoduchý příklad těla pravidla je opravdu nejzákladnější vzor, ve skutečnosti je problematika daleko složitější, tělo obsahuje daleko více parametrů a klíčových hodnot.



Obrázek 6 - Struktura Snort pravidla [vlastní zdroj]

4.3 *Formát výstrahy*

V případě, že detekční jednotka detekuje určitý typ nebezpečného kódu, vygeneruje se výstraha. Tato výstraha má svůj specifický formát. Výstižně jej zobrazil pan Radomír Orkáč ve své semestrální práci (strana 10).



Obrázek 7 - Snortem vydaná výstraha[6]

4.4 *Shrnutí*

Snort je vhodným nástrojem zabezpečení především pro menší firmy. Měl by se vzít v potaz výkon daného PC, na kterém je IDS/IPS implementováno i úložný prostor, kde budou výstrahy logovány (v řádech GB).

Pro představu je přiložena ukázka z výpisu logu, kam se ukládaly výstrahy během jednoho dne aktivního využívání připojení k internetu - viz Příloha 2.

Snort je využívám především jako open-source systém, avšak jsou i silnější komerční veze (většinou v hardwarové podobě), které nabízí mnoho různých doplňků. Zejména přesnost detekčních sond a velmi vysoký výkon detekování na rychlejší (páteřní) síti. Před zavedením IDS/IPS je nutné se zamyslet, jak silné zabezpečení společnost

[6] Zdroj: ORKÁČ, Radomír. Semestrální projekt do předmětu Směrové a přepínané sítě (2006).

potřebuje, a jestli vůbec nějaké. Implementace IDS/IPS do síťové struktury může být i otázkou v řádu statisíců korun (samotný systém, implementace, proškolení). Je potřeba vzít v úvahu poměr ceny zabezpečení a ztráty v případě napadení. Obecně je však známo, že investice do zabezpečení se vyplácí.

5 Počítačový útok obecně

Počítačové útoky mohou mít různé podoby, provádí jej různí útočníci, kteří mají různé důvody a cíle. Následující kapitoly se detailněji věnují těmto aspektům.

5.1 Počítačový útočník

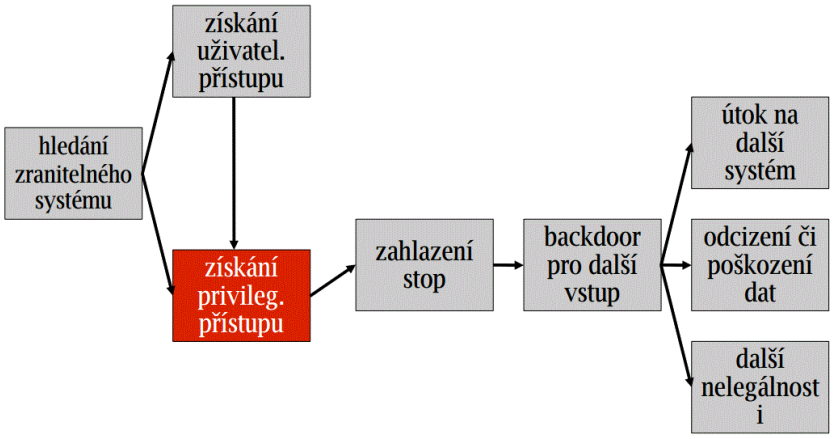
Se stále větší závislostí na počítačových systémech rostou i stále častější a důmyslnější typy útoků právě na tyto systémy. Je nutné mít na mysli, že žádný systém není stoprocentně bezpečný. Pokud je vymyšlen nový typ zabezpečení, dřív nebo později bude nalezen způsob, jak dané zabezpečení obejít. Útoky mívají různé důvody a cíle. Podle toho, jaký je důvod útoku, se útočníci dělí na hackery a crackery. [9] Ve veřejných publikacích, jako jsou zprávy a noviny, jsou často všichni chybně označováni jako hackeři. Hacker je často pouze obyčejný pracující občan, který má pouze zálibu v počítačové problematice a baví ho zkoumat, bádat a přesahovat své možnosti, v žádném případě nemá v úmyslu škodit. Oproti tomu cracker bývá specialista v daném oboru a jeho cílem je provádět počítačové útoky, především za účelem vlastního prospěchu a často i zisku, avšak není výjimkou ani provádění počítačových útoků jen pro radost a vlastní uspokojení. [9]

5.2 Důvody počítačových útoků

Metody útoků bývají stále promyšlenější. Útočníci používají různé nástroje a bezpečnostní díry v programech k dosažení svých cílů. V případě úspěchu může mít zisk velmi zajímavou hodnotou, ať už v podobě finanční nebo informační. Odhalení a dopadení konkrétního počítačového útočníka má daleko menší pravděpodobnost než při běžné loupeži. Útočníci se často skrývají za cizí IP adresy a jejich odhalení bývá často hodně náročný proces, což je také důvod, proč útoků stále přibývá. [9]

5.3 *Obecný postup útoku*

Základem provedení každého útoku je sběr informací o systému nebo službě, na kterou bude útok proveden. Tyto informace budou analyzovány a použity na přípravu útoku. Obecný postup je výstižně zobrazen na následujícím obrázku pana Satrapy z technické univerzity v Liberci.



Obrázek 8 - Obecný postup útoku[7]

Nejzákladnějším nástrojem pro sběr informací o cílovém hostiteli je pomocí Google Hacking, pomocí Google vyhledávače (v případě hledá-li útočník informace o určité společnosti nebo organizaci). [9]

V případě, že útočník připravuje útok na určitý webový portál, nejspíše využije tzv. WHOIS databáze. Celosvětová databáze serverů, které obsahují doménová jména, IP adresy, čísla portů nebo také jméno serveru, na kterém služba běží. Právě tato informace pomůže útočníkovi dále zjistit známé chyby a nedostatky daného serveru a skrz tyto chyby provést útok. [9]

Informace o vnitřní síti poskytne například nástroj Nmap. Jedná se o skenovací nástroj, pomocí kterého útočník může získat informace o IP adresách vnitřních stanic, operačních systémech, otevřených portech nebo také verzích firewallu.

Po získání dostatečného objemu informací o cílovém hostiteli útočník využívá různých technik získání přístupu skrz zabezpečení. Sociální inženýrství je jedním z nejčastějších

[7] Zdroj: http://www.nti.tul.cz/~satrapa/vyuka/site/cv/utoky.pdf

způsobů. Pokud tyto techniky nesplňují svůj účel, existují hackerské nástroje, které využívají chyb v zabezpečení. Takových nástrojů je celá řada. Tato práce se zaměřuje na určité typy, které byly vybrány jako ideální pro případ testování IDS/IPS.

6 Vybrané počítačové útoky

Vybrané počítačové útoky byly zvoleny po dohodě s odborníkem v daném oboru, panem Ing. Petrem Břehovským. Při výběru byla brána v úvahu skutečnost, že testování probíhá v laboratorních podmínkách a zohledněn výběr takových útoků na detekční systém, které by mohly splňovat hlavní cíl práce (tj. obejít bezpečnostní systém). SQL injection byl zvolen jako způsob otestování detekčních schopností IDS/IPS na incidenty z vnitřní sítě. DoS útok byl vybrán jako hrozba vnější sítě. Dále testování detekčního systému vůči šifrované komunikaci, jelikož je to věc stále častěji v síťové komunikaci využívaná.

6.1 SQL injection

Princip spočívá v tom, že útočník zadává do neošetřeného webového formuláře různé SQL dotazy. Pomocí těchto dotazů se snaží podstrčit určité vstupní hodnoty a tím zmást webový server. Úspěšným výsledkem bývá manipulace s daty v databázi nebo získání přístupu do systému.

Příklad SQL injection:

- *1 OR 1=1*
- *1' OR '1'='1*
- *1' AND 1=(SELECT COUNT(*) FROM tablenames); --*
- *'OR username IS NOT NULL OR username = '*
- *1 UNION ALL SELECT 1,2,3,4,5,6,name FROM sysObjects WHERE xtype = 'U'*
- *%31%27%20%4F%52%20%27%31%27%3D%27%31*
- *&#49&#39&#32&#79&#82&#32&#39&#49&#39&#61&#39&#49*

V případě, že by se útočníkovi podařilo proniknout tímto způsobem do systému, pochybení bývá zejména na straně programátora, který danou webovou aplikaci

vytvářel. Zabezpečit webový formulář lze například omezením velikosti vstupních hodnot, zamezením použití interpunkčních znamének nebo také počtem opakovaného zadání vstupních hodnot.

6.2 DoS (Denial of Service)

Jedná se o jeden z nejčastějších útoků zejména pro svoji účinnost a jednoduchost provedení. Princip je jednoduchý: znemožnit (odepřít) běžnému uživateli přístup k určité webové službě. Existují dva způsoby, jak lze tohoto výsledku dosáhnout.

První způsob spoléhá na to, že každý, i sebelepší a výkonnější systém, má omezenou kapacitu, ať už operační nebo paměťovou. Cílem útočníka je právě jednu z těchto kapacit zahltit takovým způsobem, aby donutil systém k restartu a tudíž znemožnil přístup k webové službě pro běžného uživatele. Druhá způsob spočívá v obsazení komunikačního média, tak aby běžný uživatel neměl přístup k webové službě. K tomu musí mít útočník zpravidla silnější datovou linku, než uživatel pokoušející se o připojení.

K těmto dvěma metodám znemožnění používání webové služby existuje několik variant, jak toho docílit.

6.2.1 Záplavový útok (SYN Flood Attack)

K tomu, aby útočník dosáhl maximálního účinku tohoto útoku, je potřeba "pouze" silnější datové linky. Pokud tento požadavek útočník není schopen splnit, může využít více slabších linek, tento postup je však složitější a náročnější. Žádoucím výsledkem je tedy znepřístupnění linky ostatním uživatelům. Názorným příkladem může být dopravní zácpa, což znamená kolona stojích aut bez možnosti projetí. Jedinou možností správce webu, kterému uniká ve většině případů zisk, je kontaktovat poskytovatele, aby zablokoval útočníkovu IP adresu. Útočník však má možnost zfalšovat svoji IP adresu a útok může pokračovat. [10]

6.2.2 Vyčerpání zdrojů

Jak už bylo řečeno, každý systém je omezen určitou kapacitou, ať operační nebo paměťovou. To znamená, že systém je schopný obsloužit pouze určitý počet dotazů za určitý čas. Právě tyto kapacity jsou útočníkovým cílem. Pokud útočník zahltí systém

množstvím nebo velikostí svých dotazů, systém již nedokáže poskytnout své služby legitimním uživatelům. Ukázkovým příkladem může být e-mailová schránka. Má určitou kapacitu a v případě, že se útočník pomocí generátoru e-mailů rozhodne schránku zahltit, není moc šancí jak mu v tom zabránit. Schránka sice obsahuje filtry pro filtrování příchozí pošty, ale pokud generátor vytváří zprávy různých zdrojů s různým předmětem, filtry jsou v tuto chvíli prakticky nepoužitelné. Zdánlivou šancí může být kontaktování poskytovatele o zablokování dané IP adresy útočníka, což ale útočníkovi nebrání v tom, zfalšovat svojí IP adresu a pokračovat v útoku.[11] Většinou majiteli e-mailové schránky nezbývá nic jiného, než se dané schránky vzdát a založit si novou.

6.2.3 Útok využívající chybu v SW nebo HW

Obecně se říká, že nikdo není neomylný. Toto platí i v případě programátorů. Jak už sám název napovídá, cílem útočníka jsou chyby v softwarovém nebo hardwarovém vybavení. Tyto chyby jsou buď obecně známé, a pokud na ně není vydána záplata, tak je systém lehce zranitelný, a nebo útočník skenováním daného systému přijde na určitou skulinu, kterou využije, aby pronikl do systému. Cílem takového průniku v případě DoS útoku je zacyklení nebo dokonce zhroucení systému. Výsledek je tedy opět stejný, běžný uživatel nemá přístup k požadované službě. [10]

6.2.4 Napadení DNS

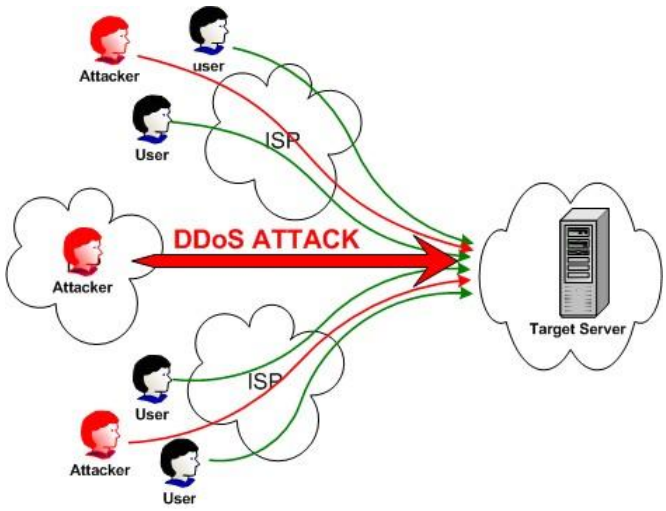
Princip toho útoku je v přepsání serverové DNS tabulky. Pozměnit IP adresy, ať už ve prospěch útočníka nebo do tzv. slepé uličky, kdy je v DNS tabulce zadána IP adresa "nikam".

Při navázání spojení zdrojový počítač vysílá SYN paket na cílový počítač. Cílový počítač naslouchá na otevřeném portu a přijímá právě tyto SYN pakety. Pokud přijme SYN paket, odpovídá SYN/ACK zpět ke zdrojovému počítači. Ten daný paket přijme, vysílá ACK, což se jedná o uskutečnění spojení mezi oběma body.

Princip útoku spočívá v tom, že útočník zamění právě zdrojovou adresu a tudíž SYN/ACK nemá kam dorazit. V tomto stavu čeká, dokud nevyprší tzv. čekací doba, což bývá až 23 minut.[9] To je dost dlouhá doba na to, aby útočník zahltil svoji oběť dotazy.

6.3 DDoS

V podstatě se jedná o rozšíření DoS útoku. Toho rozšíření spočívá v tom, že útoky jsou Distribuované z více směrů, většinou prostřednictvím více útočníků, avšak není to pravidlem. Tyto více-směrové útoky může ovládat jeden útočník skrz tzv. zombie počítače. Počítače obyčejných uživatelů jsou napadeny a zneužity pro tento druh útoku, hovoříme zde o tzv. zombie síti. [10] DDoS útok je podstatně složitější na organizaci a znalostní dovednosti útočníka (útočníků), ale efektivita takového útoku se několikrát násobí a zpravidla je i velmi obtížné, skoro až nemožné, dohledat původce útoku.



Obrázek 9 - DDoS útok[8]

6.3.1 Obrana

Bránit se DoS (případně DDoS) útokům není vůbec jednoduché, někdy skoro až nemožné. Základním pravidlem obrany, jako u většiny útoků, je pravidelná aktualizace operačního systému a bezpečnostních nástrojů. Dále se doporučuje: používat kvalitní síťové připojení s dostatečnou přenosovou kapacitou; zakázat vpuštění prvního paketu do sítě, zejména proti útokům DDoS, které často falšují IP adresu (při legitimní komunikaci se TCP paket posílá dvakrát); v případě UDP zamezit přístupu zvenčí (nikoliv z vnitřní sítě, protože protokol UDP mohou používat i legitimní aplikace); blokovat nepotřebné služby; zálohovat. Také se vyplatí připravit si případný krizový plán, pokud by skutečně k útoku došlo. [11]

[8] Zdroj: http://imgcdn.priyo.com/201303/ddos-attack-30313-460.jpg

6.4 Zašifrovaný přenos

Šifrovaná síťová komunikace sice nepatří mezi běžné typy počítačových útoků, jde však o jednu z možností, jak se vyhnout bezpečnostním opatřením.

Obecně SSL komunikace pracuje na principu asymetrické šifry. Komunikující strany k tomu využívají dva druhy klíčů - veřejný a soukromý. Komunikace zašifrovaná veřejným klíčem zajišťuje bezpečný přenos informací a rozšifrovat jej dokáže pouze majitel soukromého klíče. Pokud bezpečnostní zařízení nevlastní tyto klíče, není schopný detekovat zašifrovaný přenos a to může být způsob jak obejít IDS/IPS.

II. Praktická část

7 Sestavení sítě

K testování bezpečnostního systému je potřeba sestavení topologie sítě. Síť byla rekonstruována na zařízeních využívaných k výuce informačních technologií na Jihočeské univerzitě. Jedná se o profesionální síťové zařízení společnosti Cisco. Maximální výkonnost samotných síťových zařízení, stejně jako PC sestavy, kde je testování prováděno, ovlivňuje celý testovací proces.

PC

Intel Core 2 Duo - E6850 3.00GHz

RAM 1.00GB

Cisco zařízení

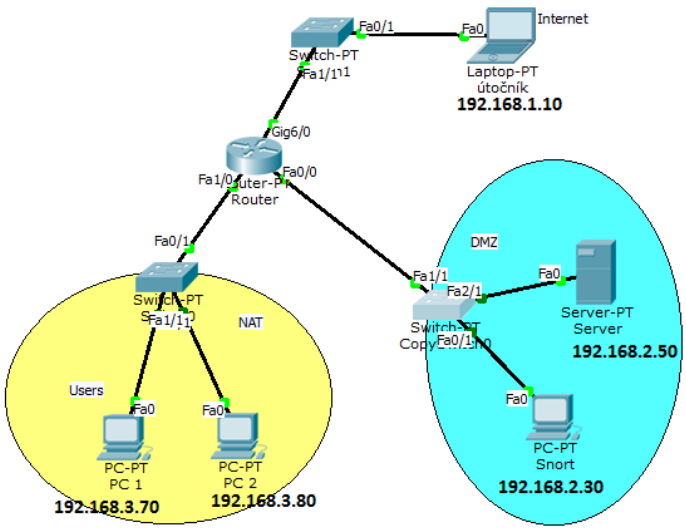
Switch

Cisco Catalyst 2960 24 10/100

Router (MLS)

Cisco Catalyst 3560V2 24 10/100 PoE + 2 SFP

7.1 Schéma zapojení



Obrázek 10 - Schéma zapojení[vlastní zdroj]

7.2 Postup testování

Je nutné si uvědomit, že testování probíhá v laboratorních podmínkách, což znamená bez přítomnosti skutečného reálného provozu. Tato skutečnost má výhodu v tom, že bezpečnostní systém IDS/IPS může věnovat maximální pozornost simulačním útokům a tím s maximální rychlostí odezvy. V porovnání s testováním v reálném provozu by to znamenalo, že bezpečnostní systém musí mimo simulační útoky provádět analýzu také běžného provozu dat, což může detekční rychlost systému zpomalit.

7.2.1 Spuštění Snort

Veškerý procházející provoz byl monitorován bezpečnostním systémem Snort, implementující IDS/IPS. Pozorování bylo realizováno dvěma módy: na jedné polovině obrazovky monitorování síťového provozu pomocí sniffer módu, ve druhé polovině pomocí Network IDS módu (porovnání podle pravidel). Sniffer mód spuštění pomocí příkazu:

- *.\Snort -v*

Použitím tohoto příkazu se zobrazuje veškerý procházející provoz (zobrazení všech paketů). IDS v Network módu, které bylo spuštěno pomocí příkazu:

- *.\Snort -A console -i1 -c .\Snort\etc\Snort.conf -l .\Snort\log -K ascii*

Tento mód porovnává síťový provoz na základně konfigurace v adresáři Snort.conf. Zachycené hrozby vypisuje na obrazovce a dále je loguje na disk, konkrétně do adresáře .\Snort\log . Velmi důležité je nastavení detekovaného interfacu (-iX).

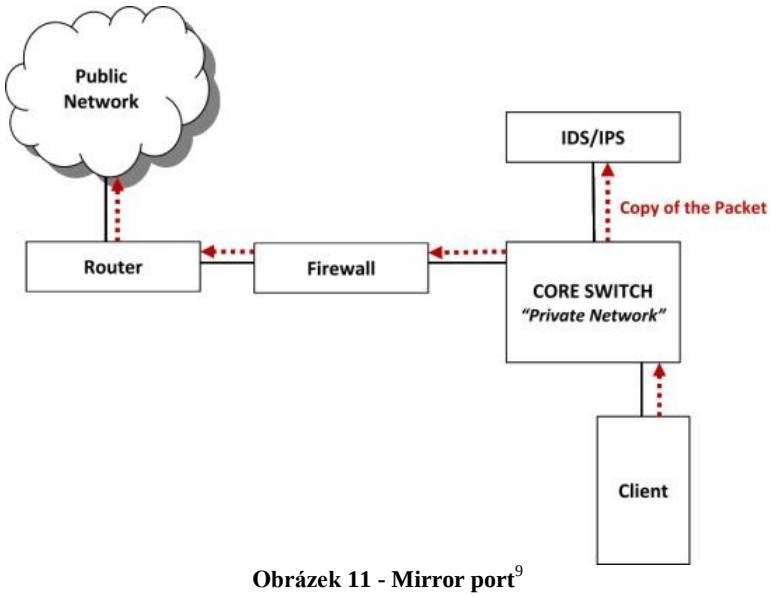
Snort využitý v této práci byl získaný z www.snort.org, tedy přímo z oficiálních stránek organizace. Snort byl stažen v nejaktuálnější nekomerční verzi 2.9.5.5. Jak už bylo řečeno, pracuje zejména podle předem daných pravidel, a právě tato pravidla bylo nutné také získat z oficiálních stránek společnosti, opět v nejaktuálnější verzi označené jako 2955. Následnou konfigurací - viz Příloha 1, byl uveden bezpečnostní systém do provozu.

7.2.2 Potřebné nástroje

Po sestavení modelové sítě a nastavení bezpečnostního systému byly nutné konfigurace dalších potřebných nástrojů.

Další velmi důležitým nástrojem v topologii je Multi-Server Simulator. Tento nekomerční nástroj, vytvořený společností Paessler, byl stažen z oficiálních stránek organizace www.paessler.com ve verzi 0.1, což je verze vydaná 26. 5. 2009. Tento nástroj, simulující server s otevřenými porty, slouží jako cíl útoků (v topologii se jedná o PC s IP adresou 192.168.2.50). Tento softwarový Multi-Server umožňuje spuštění služeb jako HTTP, SMTP, DNS, FTP, SNMP nebo nastavení jakéhokoliv otevřeného portu.

Na počítači označeném jako útočník (PC a IP adresou 192.168.1.10) jsou konfigurovány nástroje umožňující skenování vnitřní sítě (Nmap) a následnou realizaci útoků (Hping3, Burp Suite, OpenSSL, OpenVPN). Tato činnost v síti je kontrolována bezpečnostním systémem a dále vyhodnocována. K tomu, aby byla zajištěna kontrola napříč celou vnitřní topologií sítě, je veškerý provoz kopírován na tzv. mirror port (v Cisco označováno jako SPAN port).



Obrázek 11 - Mirror port[9]

[9] Zdroj: https://ia.signal.army.mil/IAF/images/IDS.jpg

Na tomto portu je připojený PC s bezpečnostním systémem Snort, a právě na tento port je kopírován veškerý provoz v síti. Konfigurace mirror portu:

- Switch(config)# no monitor session 1
- Switch(config)# monitor session 1 destination interface fastEthernet0/1
- Switch(config)# monitor session 1 source interface fastEthernet1/1
- Switch(config)# monitor session 1 source interface gigaEthernet2/1
- Switch(config)# end

Provoz na portech označené jako FastEthernet1/1 a FastEthernet2/1 je kopírován na FastEthernet0/1. Takto nastavený mirror port je schopný detekovat hrozby v oblasti vlastní VLAN. V případě detekce nežádoucích aktivit z jiné VLAN, než kde je nasazeno IDS/IPS, je nutné provést rozšířenou konfiguraci mirror portu.

Skenování vnitřní sítě umožňuje program zvaný Nmap. Tento program je nekomerčně dostupný a hodí se k testování pozornosti bezpečnostního systému vůči skenování vnitřní sítě. Lze jej získat z oficiálních internetových stránek organizace a to na www.nmap.org.

Pro testování útoků přicházejících z vnější sítě, byl vybrán nástroj Hping3, který realizuje DoS útok, konkrétně SYN flood. Tento typ útoku proti bezpečnostnímu systému byl vybrán pro svoji efektivitu a hojné využití v praxi.

Pro otestování schopnosti detekovat nežádoucí činnost uvnitř sítě byla vybrána metoda SQL injection, a to především z důvodu rozšířeného použití v praxi. SQL injection je realizováno pomocí nástroje Burp Suite Professional verze 1.5.

Poslední část testování se věnuje detekční schopnosti IDS/IPS vůči šifrované komunikaci. K tomu je využit nástroj OpenSSL (verze 1.0.1e). Tento nástroj generuje šifrovací klíče a díky tomu je možné provést zašifrování síťové komunikace. Je možné jej získat z oficiálních stránek organizace www.openssl.org. Pro potvrzení získaných výsledků prostřednictvím OpenSSL, byl využit nástroj OpenVPN (verze 5), pomocí kterého je možné vytvořit šifrovaný tunel mezi dvěma počítači. Opět je možné jej stáhnout z oficiálních stránek organizace www.openvpn.net.

8 Testování

Tato práce se zaměřuje pouze na nástroje prakticky ověřené a vyzkoušené. Jsou dalších nástroje, které lze využít, avšak právě tyto byly vybrány k účinnému otestování bezpečnostního systému IDS/IPS po dohodě s panem Ing. Petrem Břehovským.

8.1 Skenování cíle

Nmap je především skenovací nástroj, který umí získat informace o určité síti. Je schopný získat informace o dostupnosti počítačů v síti, operačních systémech, jež na nich pracují, verze serverů nebo firewallů atd. Výhodou je open-source distribuce a také implementace na velký počet systémových platforem (Lunix, Solaris, Mac OS, Windows atd.), což také přidává na uživatelské oblíbenosti. Touto prací využitý Nmap (verze 6.40) pracuje pod systémem Windows, který s společně s grafickou podporou je nazýván Zenmap.

8.1.1 Nejzákladnější techniky skenování

TCP connect() scan [-sT]

Jedná se o skenování vzdálené sítě pomocí protokolu TCP, kdy systém navazuje TCP spojení. Jde o efektivní způsob skenování, avšak velmi lehce detekovatelný firewallem nebo systémem IDS/IPS.

Příklad:

- *nmap -sT 192-168.2.50*

SYN stealth scan [-sS]

V principu jde o stejný způsob jako TCP connect. Nmap sice pošle paket SYN na připojení ke službě, ale pokud vzdálený hostitel odpoví paketem SYN/ACK, nmap spojení RST paketem ukončí.

Příklad:

- *nmap -sS -O 192.168.2.50*

Ping scan [-sP]

Jak již z názvu vyplývá, tato metoda má velmi blízko ke klasickému ping příkazu (protokol ICMP). Zdroj posílá paket Echo request a čeká na odpověď vzdáleného hostitele paketem ECHO reply.

Příklad:

- *nmap -sP 192.168.2.50*

UDP scan [-sU]

UDP není stavový protokol. Paket poslaný na určitý port je v případě žádné odpovědi považován za otevřený, v případě přijmutí ICMP port unreachable je port zavřený. Kvůli této vlastnosti skenování dosahuje velkých rychlostí, výhodu tedy může přinést, pokud je potřeba skenovat velké množství portů nebo adres.

Příklad:

- *nmap -sU 192.168.2.50*

Timing template [-sS -Tx]

Umožňuje velmi rychle nebo naopak velmi pomalu odesílání paketů. Záleží na nastavení parametru Tx (0-5), kdy T0 značí rozmezí mezi dvěma pakety až 5 minut, naopak nastavení parametru T5 zapříčiní velmi rychlé odpovědi (v řádech milisekund). Obecně platí, čím delší časové rozmezí, tím vetší šance vyhnout se detekčnímu systému.

Příklad:

- *nmap -sS -T5 192.168.2.50*

Další techniky

Další typy TCP skenů jako jsou Windows scan, ACK scan, FIN scan, NULL scan, List scan atd. a rozšířené techniky skenování vzdáleného hostitele, aby nedošlo k odhalení detekčním systémem.

- Fast scan [-F] - skenování pouze známých portů (soubor vedený Nmapem)
- Use Decoy [-D] – definice náhodných IP adres a mezi nimi ukrytá vlastní adresa

- Time to live [--ttl] – určí hodnotu TTL, která bude paketu nastavena
- Packet Trace [--packet-trace] – zobrazí každý odeslaný i příchozí paket
- Random scan [-r] – odesílání paketů v náhodném pořadí
- --data-length – úprava velikosti paketu (například velikost 1337)

Ve všech zmíněných případech skenování byla odezva IDS totožná, vydání výstrahy portscan.

11/10-22:00:34.353705 [**] [122:1:1] (portscan) TCP Portscan [**] [Classification: Attempted Information Leak] [Priority: 2] {PROTO:255} 192.168.1.10 -> 192.168.2.50

Největší množství výstrah, bezpečnostním systémem přímo označeno jako DoS útok, způsobilo tzv. Fragment IP pakets [-f]. Tato metoda skenování rozděluje TCP hlavičku na několik samostatných paketů. Důležité je, že byl nalezen způsob, jak se vyhnout detekci bezpečnostním systémem. Jediný typ skenování, pomocí nástroje Nmap, který nevzbudil pozornost IDS, je Idle proxy scan.

8.1.2 Idle proxy scan [-sI]

Tento typ scanu úspěšně obešel IDS sondu pomocí ukrytí své identity za jinou. Tomuto typu scanu se říká také zombie scan. Jeho úkolem je schovat se za identitu jedno ze zařízení ve vzdálené skenované síti (například tiskárna). Nmap pošle SYN ACK paket a zařízení vnitřní sítě samozřejmě odpoví RST (reset). Nmap z toho RST paketu však odcizí ID, což je identifikace zařízení vnitřní sítě. Poté je zaměněno vlastní ID za odcizené ID a komunikace tak prochází bez povšimnutí.

Příklad:

- *nmap -sI 192.168.1.7 192.168.2.50*

8.1.3 Shrnutí

Během testování byly použity různé metody skenování. Odesílání paketů různých protokolů (UDP, TCP, ICMP), také časování, úprava délky a velikosti, odesílání paketů v náhodném pořadí atd. Všechny takto upravené pakety, s cílem získat určité informace o vzdáleném hostiteli, byly odhaleny detekčním systémem a zapsány do logu. Největší

pozornost vzbudila fragmentace paketů, detekčním systémem označena přímo jako Denial of Service (DoS). Naopak jediným nedetekovaným způsobem, jak získat informace o vzdáleném hostiteli pomocí nástroje Nmap, byl Idle proxy scan, kdy skenovací nástroj Nmap ukryl vlastní identitu za identitu jiného zařízení ze vzdálené sítě.

8.2 SYN flood attack

Realizováno nástrojem Hping, což je velmi užitečný software pro testování odolnosti počítačových sítí. Jeho úlohou je odesílání paketů v různých formátech (TCP, UDP, ICMP). Jak už sám název napovídá, Hping má velice blízko k ping. Rozdílem je skutečnost, že Hping má daleko širší škálu možností, jako například traceroute mód nebo správu odesílaných paketů. K otestování bezpečnostního systému byla vybrána verze Hping3. Jedná se o linuxovou verzi. V případě Windows by byla zvolena verze Hping2, která byla vytvořena přímo pro Windows s 32-bitovým systémem.

Pomocí Hping3 byl proveden útok zvaný SYN flood attack, nebo-li záplavový útok, na serverový počítač (PC s IP adresou 192.168.2.50). Na PC s bezpečnostním systémem Snort (PC s IP adresou 192.168.1.30), byl zachytáván síťový provoz a případě detekce, zobrazení a zapisování do logu. SYN flood attack byl proveden příkazem:

hping3 -i 1 -S -p 80 192.168.2.50

IP adresa - cílový hostitel

-p 80 - port, na který je proveden útok

-i 1 - vteřina mezi každým odeslaným paketem

-S - SYN flag, což znamená odeslání pouze paketu SYN pro navázání spojení (viz. kapitola TCP connect)

Testování bezpečnostního systému začalo generováním paketů po jedné vteřině - nastavením parametru -i1. IDS zachytil provoz pomocí sniffer módu, avšak podle NIDS módu není potencionální hrozbou. Stejný výsledek je možné pozorovat při nastavení časového parametru generování na 10 paketů za vteřinu, 100 paketů za vteřinu, 1000 za vteřinu i dokonce 10 000 paketů za vteřinu. Výsledek je vždy stejný, sniffer mód monitoruje provoz každého paketu, ale detekce podle pravidel nehlásí žádnou hrozbu.

Změna přichází, pokud na časovém parametru nastavíme hodnotu -i u10, což znamená generování 100 000 paketů za vteřinu. Toto nastavení již nevyhovuje legitimní komunikaci a je na tento provoz upozorněno generováním výstrahy v následující podobě:

11/18-19:37:20.851920 [**] [129:15:1] Reset outside window [**] [Classification: Potentionally Bad Traffic] [Priority: 2] {TCP} 192.168.1.10:35918 -> 192.168.2.50:80

Stejná výstraha byla vypsána i při generování paketů rychlostí -i u1 (1 000 000 paketů za vteřinu). Hranici reagování Snortu na rychlost provozu lze regulovat v konfiguračním souboru parametrem stream5, kde pro každý protokol je nastavená jiná maximální hodnota legitimního provozu.

Zajímavostí je, že po realizaci -i u10 (100 000 paketů za vteřinu) si Snort zapamatovává zdrojovou IP adresu, ze které tento útok přichází. Pozdější testování pomalejšího generování provozu, které původně zůstalo nepovšimnuto, se v této chvíli stává také potenciálně nebezpečným. Hodnocení dané adresy opět běžným způsobem přichází až po 180 vteřinách. Tato hodnota je defaultně nastavena v konfiguračním souboru a je možné ji změnit.

8.2.1 Shrnutí

Otestováním bezpečnostního systému IDS proti DoS útoku (SYN flood attack) pomocí nástroje Hping3 bylo zjištěno, že systém zvládá zpracování a vyhodnocení velkého objemu dat. Výsledek testování je takový, že pokud Snort považuje komunikaci za potenciálně nebezpečnou, tak zdrojovou IP adresu zapíše do logu s příslušnou výstrahou a dále tuto IP adresu monitoruje. Na provoz z této IP adresy je upozorněno, i když se jedná o legitimní komunikaci. Po uplynutí 180 vteřin začne bezpečnostní systém vyhodnocovat danou adresu stejným způsobem jako před vydáním výstrahy.

8.3 SQL injection

Provedení SQL injection proběhlo pomocí nástroje Burp Suite, což je víceúčelový software, který zvládá celý proces testování webové aplikace. Je možné jej využít od počátečního zmapování, provedení analýzy a následného proniknutí skrz nedokonale zabezpečenou webovou aplikaci. Velkou výhodou je jeho automatizovaná činnost, která

dokáže kombinovat několik technik útoku za velmi krátkou dobu. Tím je samotný útok a celkové testování webové aplikace daleko rychlejší a efektivnější.

SQL injection je využit v této práci jako útok z vnitřní sítě, kdy je předmětem testování, jestli bezpečnostní systém IDS zareaguje na nebezpečný incident ve vnitřní síti. K tomu, aby bylo možné realizovat útok SQL injection, bylo potřeba webové aplikace, která bude připojena na databázi. Nejideálnějším příkladem je přihlašovací portál na webových stránkách. Tato webová aplikace byla naprogramována jako soukromá externí práce a poté byla využita čistě pro testování tohoto druhu útoku. Webová aplikace běží na webserveru Wamp společně s MySQL databází.

Obrázek 12 - vlastní webaplikace [vlastní zdroj]

Prvotní testování reakce detekčního systému na SQL injection byla bez odezvy. Postupným pátráním proč tomu tak je bylo zjištěno, že pravidla pro detekci SQL injection jsou v základní konfiguraci primárně určeny na podněty přicházející z vnější sítě (nastavením zdrojové IP adresy jako $EXTERNAL_NET).

Aby bylo možné detekovat podněty přicházející i z vnitřní sítě, je nutné vytvořit nový soubor s těmito pravidly a proměnnou $EXTERNAL_NET přepsat na $HOME_NET. Poté v konfiguračním souboru Snortu (Snort.conf) definovat nový soubor s pravidly. Tímto bude zajištěna detekce SQL injection i pro uživatele vnitřní sítě.

Po spuštění nástroje Burp a realizaci SQL injection na webovou aplikaci IDS detekuje nežádoucí činnost a Snort vydává výstrahy.

Příklad situace, kdy bezpečnostní systém detekuje SQL injection, které obsahuje v řetězci znaménko + (plus):

12/3-20:0:36276743 [**] [1:9017:2] SQL Injection - General - PLUS [**] [Classification: Web application Attack] [Priority: 1] {TCP} 192.168.1.10:2817 -> 192.168.2.50:80

Další detekované hrozby měly podoby

- SQL injection - General - GET
- SQL injection - General - AND
- SQL injection - General - OR
- SQL injection - General - UNION
- SQL injection - General - SELECT

nebo řetězce, které obsahovaly nežádoucí znaky (\,/,:,%,?,;), generovaly výstrahu

- The system detected SQL injection Attack

8.3.1 Shrnutí

Burp, jako nástroj pro testování webových aplikací, obsahuje rozsáhlou databázi řetězců, které využívá k prolomení zabezpečení webové aplikace. Výsledek testování odolnosti IDS proti útoku SQL injection je takový, že nebyl nalezen způsob, který by mohl být vůči webové aplikaci nebezpečný a bezpečnostní systém jej nedetekoval.

8.4 Šifrovaný přenos informací

Jelikož je komunikace šifrována, detekční schopnost IDS nemá šanci zašifrovaný škodlivý kód detekovat. Snort, jakožto bezpečností systém, nemá soukromý klíč k dešifrování a veřejný klíč k opětovnému zašifrování komunikace. Další věcí a pouhou úvahou je časová náročnost – pokud by bylo možné komunikaci rozšifrovat, analyzovat, vyhodnotit všemi možnými způsoby detekování (podle vzoru, anomálie, odchylky) a znovu zašifrovat, způsobilo by to velkou časovou odezvu. Jsou IDS/IPS, které obsahují vysokorychlostní dekodéry, ale jedná se spíše o nákladné komerční nástroje.

8.4.1 Zajištění šifrovaného přenosu

K zajištění šifrované komunikace je využit nástroj OpenSSL. Ještě předtím než začne probíhat samotný zabezpečený přenos, je nutné, aby si obě komunikující strany vyměnily kryptografické algoritmy. Výměna klíčů může být zajištěna například pomocí RSA nebo DSA algoritmu. Dále je potřeba definovat, jakým způsobem bude probíhat symetrická šifra, typicky pomocí AES nebo DES šifrování. V neposlední řadě také to, jaká bude použita hash funkce, standardem bývá MD5 nebo SHA.[13]

Než se mohla testovat detekční schopnost IDS vůči šifrované komunikaci, bylo nutné pomocí OpenSSL vytvořit šifrovací klíče. Výchozí nastavení generování klíčů je o velikosti 1024 bitů a pomocí hash funkce SHA. Samotné generování bylo provedeno následujícím způsobem:

- req -new -config .\conf\openssl.conf -out test.csr
- rsa -in privkey.pem -out test.key
- x509 -in test.csr -out test.crt -req -signkey test.key -days 365

Po vygenerování klíčů, potřebných k šifrovanému přenosu, je potřeba upravit konfiguraci webserveru, tj. povolit naslouchání serveru na portu 443 a tím umožnit komunikaci přes SSL.

Samotné testování proběhlo na již zmíněné soukromé web aplikaci, kde při načtení webu v podobě HTTP byla generována výstraha v podobě přenášení citlivých údajů napříč sítí. Tato výstraha byla způsobena uvedením e-mailové adresy v zápatí webové aplikace.

12/3-20:33:46.298364 [**] [138:5:1] SENSITIVE-DATA Email Addresses [**] [Classification: Sensitive Data was Transmitted Across the Network] [Priority: 2] {TCP} 192.168.1.10:2821 -> 192.168.2.50:80

Výsledek šifrovaného přenosu (HTTPS) byl takový, že IDS nedetekoval tento incident a negeneroval žádnou výstrahu. Komunikace v šifrované podobě, ačkoliv obsahovala potencionálně škodlivý kód, prošla skrz IDS bez povšimnutí a bez vydání výstrahy.

8.5 Zašifrovaný tunel

Po úspěšném proniknutí šifrované komunikace pomocí HTTPS a zjištění, že bezpečnostní systém není schopný detekovat zašifrovaný přenos, byl využit nástroj OpenVPN k vytvoření šifrovaného tunelu mezi dvěma počítači. Tímto způsobem zajistit, aby veškerá komunikace mezi dvěma body byla šifrována a tím pádem nedetekována.

K vytvoření šifrovaného tunelu je potřeba jednoho generovaného klíče, který musí mít obě strany stejný. Samotná konfigurace už je jednoduchou záležitostí. Jde pouze o to na obou stranách nastavit IP adresu protějšku, port a protokol, přes který budou komunikovat. Po realizaci tunelu se vytvoří nové spojení (s novou IP adresou) téměř odpovídající propojení dvou počítačů pomocí síťového kabelu.

Základní konfigurace na straně serveru a na straně klienta

proto udp	proto udp
remote 192.168.2.50 53	remote192.168.1.10 53
secret klic.key	secret klic.key

Takto vytvořený tunel umožňuje komunikovat mezi dvěma počítači (z vnitřní sítě do vnější a naopak) prostřednictvím šifrované komunikace. Uživatel může přenášet a modifikovat data nebo realizovat počítačové útoky do vnitřní sítě na cílového hostitele bez povšimnutí bezpečnostního systému, lze tedy hovořit o stoprocentním přechytračení IDS.

8.6 *Přehled testování*

Přehled získaných výsledků z provedených experimentů.

Metoda	Nástroj	Detekováno	Výstraha	Podmínky
Skenování sítě	Zenmap	ano/ne	*[**] [122:1:1] (portscan) TCP Portscan [**] [Classification: Attempted Information Leak] [Priority: 2] {PROTO:255}*	Všechny metody skenování cílového hostitele detekovány až na jedinou - Idle proxy scan (získání ID zařízení vnitřní sítě a ukrytí se za něj)
DoS (Denial of Service) - SYN flood attack	Hping3	ano	*[**] [129:15:1] Reset outside window [**] [Classification: Potentionally Bad Traffic] [Priority: 2] {TCP}*	Detekování při vyšší rychlosti generování paketů a zapamatování útočící IP adresy
SQL injection attack	Burp Suite	ano	[**] [1:9017:2] SQL Injection - General - ALL [**] [Classification: Web application Attack] [Priority: 1] {TCP}	Detekováno a vydána výstraha o jaký přesný SQL injection útok se jedná
SSL (Secure Sockets Layer)	OpenSSL	ne	žádná	Potencionálně nebezečná komunikace nebyla po zajištění šifrovaného přenosu detekována
VPN (Virtual Private network)	OpenVPN	ne	žádná	Vytvořením tunelu pro šifrovanou komunikaci lze provádět jakékoliv dříve použité útoky a bez detekování

Obrázek 13 - Přehled získaných výsledků[vlastní zdroj]

9 Implementace IPS

V poslední době se čím dál častěji ve veřejných publikacích objevuje IDS/IPS označeno jako IDPS (Intrusion Detection Prevention System). Takovéto označení se začalo používat především proto, aby se ukázalo, jak velice jsou si oba systémy blízko, že je lze považovat za téměř jednotný systém. Toto ovšem platí především u komerčních produktů, které mají zpravidla vlastní operační systém. V případě této práce a použití nástroje Snort není možná konfigurace IPS na operačním systému Windows. Na tento operační systém není dostupný žádný nekomerční paketový filtr, který by se Snortem

dokázal spolupracovat, pouze paketový zachytávač (Winpcap), který dokáže pouze pasivně reagovat na podněty. Touto pasivní reakcí je myšleno použít, místo výchozí konfigurace pravidel nastavené jako ALERT, způsob REJECT.

REJECT, v případě detekce potenciálně nebezpečného TCP paketu, generuje "TCP reset" nebo v případě zachycení protokolu UDP, odpovídá "ICMP unreachable port" a tím bude daná komunikace zastavena.

Při nasazení Snortu na operačním systému Linux je možné konfigurace aktivní odezvy podstatně rozšířená, jelikož lze využít nástroj iptables (paketový filtr) a tím zajistit aktivní ochranu sítě pomocí IPS.

10 Optimální nasazení IDS/IPS

Při zvažování, jak zvolit optimální nasazení IDS/IPS v síti, by správce bezpečnosti měl mít na mysli tu nejdůležitější otázku, zda je vůbec potřeba nasazení IDS/IPS v síti. Pokud ano, jakou investici vložit do tohoto druhu zabezpečení. Při využití nekomerčního Snortu je minimální nutností proškolení zaměstnanců, kteří budou, v případě IDS, sledovat odezvy systému v logu a vyhodnocovat záznamy. V případě IPS je potřeba zvážit, jaké důsledky bude mít pro společnost zamezení legitimního provozu. Dále také, jaké snížení výkonu sítě způsobí nasazení IDS/IPS (především na páteřních spojích).

Výběr optimálního nasazení IDS/IPS rozhodně není jednoznačnou záležitostí a je potřeba zvážit mnoho faktorů. Tento návrh optimálního nasazení se zaměřuje na topologii sítě, která byla využita v testování bezpečnostního systému, a je nutné si uvědomit, že na jiné topologie s jinou strukturou, může být nasazení IDS/IPS o poznání rozdílné.

10.1 Umístění v síti

K optimálnímu nasazení IDS/IPS v síti byly vybrány a odzkoušeny dvě základní varianty, které odpovídají bezpečnostním požadavkům. Základní myšlenkou nasazení IDS/IPS v síti je, aby byl systém ukryt za firewallem. Až v případě, že by hrozba prošla

skrz firewall, je na systému IDS/IPS tuto hrozbu odhalit. Tímto způsobem se dá též kontrolovat propustnost firewallu a případně poupravit jeho nastavení.

První varianta s jedním IDS/IPS v síti - viz. Příloha 3, je složitější především konfigurací síťové komunikace, kdy je potřeba správně nastavit kopírování paketů tak, aby veškerá komunikace byla analyzována IDS/IPS. K tomu je potřeba směrovat komunikaci skrz dvě síťové zařízení a to má vliv na záplavu sítě kopírovanými pakety. Problém by nastal v případě, pokud by VLAN byla konfigurována jako NAT. Při útoku z vnitřní sítě by IDS/IPS detekoval útok skrz společnou adresu, tudíž na neznámém koncovém uživateli. Z toho vyplývá, pokud by se měl zvolit tento druh nasazení IDS/IPS a tím ušetřit finanční prostředky, z hlediska vyššího úrovně zabezpečení by v síti neměl být konfigurován NAT.

Druhá možnost nasazení IDS/IPS - viz. Příloha 4, kdy bezpečnostní systém se nachází v každé VLAN síti zvlášť. Z pohledu přehlednosti o aktivitách v každé jednotlivé síti a celkovému zabezpečení se zdá být tato varianta lepší, avšak z pohledu nákladů dražší. V počátečním sestavení náročná konfigurace, protože je nutné implementovat bezpečnostní systém do každé VLAN sítě zvlášť, ale zároveň každý bezpečnostní systém může být konfigurován podle potřeby konkrétní sítě.

10.2 Volba systému

Jak už bylo řečeno, IDS se od IPS liší svým pasivním přístupem. Právě tento pasivní přístup může být v určitých případech užitečnější, než právě aktivita IPS. Jde o konfiguraci, kdy je nutné zvážit, zda hlásit i sebemenší odchylku od běžného provozu nebo dát komunikaci jakýsi volnější průchod s tím, že může určitý škodlivý kód projít bez povšimnutí skrz zabezpečení. V případě sítě, kde je implementován systém IDS, může být konfigurace zabezpečení přísnější. Správce bezpečnosti, který kontroluje aktivitu, může danou komunikaci posoudit, avšak bude mít větší objem dat k vyhodnocování. V případě IPS je nutné zvážit, jaké následky bude mít zamezení legitimní komunikace pro organizaci, která je právě tímto systémem chráněna. Při zvolení IPS, musí být navrhnuta co nejvhodněji a s určitým citem konfigurace pravidel.

10.3 Návrh optimálního nasazení bezpečnostního systému

Po dlouhém testování a zvážení zmíněných kladů a záporů by optimální síť měla obsahovat co nejvhodněji navrženou konfiguraci IDS/IPS právě pro konkrétní síť. Tento systém by měl být nasazen za firewallem (Network-based) a na kritických místech sítě (Host-based). Důležité je, aby byl na konkrétní topologii dlouhodobě testován a laděn pro svoji optimální funkčnost (nejlépe 100% zamezených útoků a 0% přerušené legitimní komunikace). Tato varianta je finančně i časově velmi náročná. V případě, že by jeden z těchto faktorů chyběl, je nutné implementovat bezpečnostní systém, a to buď prvním způsobem nasazení (umístění jednoho IDS/IPS pro celou topologii) nebo minimálně do VLAN sítě, kde je největší pravděpodobnost útoku (umístění serveru). Optimální nasazení IDS/IPS v grafické podobě - viz Příloha 5. Vždy však záleží na kombinaci všech bezpečnostních nástrojů, nastavení celkové bezpečnostní politiky a hlavně je důležité mít na mysli, že nejlepším bezpečnostním nástrojem je lidský mozek.

Závěr

Hlavním cílem bakalářské práce bylo nalézt způsob, jak obejít bezpečnostní systém IDS/IPS. Ke splnění tohoto cíle bylo potřeba rozsáhlého experimentování a zkoumání, jaký typ počítačového útoku bude schopný obejít bezpečnostní systém.

Během testování byly nalezeny zajímavé výsledky, které mohou sloužit jako upozornění pro bezpečnostní správce, kteří k zabezpečení využívají Snort.

První testování proběhlo vůči nástroji Nmap, jelikož se jedná o jeden z nejrozšířenějších skenovacích programů. Experimentováním byl nalezen způsob, jak obejít IDS/IPS. Tento způsob přechytračení bezpečnostního systému spočívá ve zneužití identifikačního čísla zařízení skenované sítě, pod nímž je ukryta vlastní identity. Další zajímavý výsledek byl získán při realizaci útoku SYN flood, kdy IDS/IPS si zapamatovává IP adresu, ze které hrozí nebezpečí. Na tuto IP adresu bylo upozorněno, i když se jednalo o legitimní komunikaci. Hlubším zkoumáním bylo zjištěno, za jakých podmínek a na jak dlouho si bezpečnostní systém danou IP adresu pamatuje, než byla komunikace z této IP adresy opět vyhodnocována běžným způsobem. Útok SQL injection byl využit jako test IDS/IPS, zda je schopný detekovat bezpečnostní hrozby ve vnitřní síti. K tomuto typu útoku byla využita vlastní naprogramovaná web aplikace, aby bylo možné provádět důkladné testování, různé experimentování a byla znemožněna možnost právního stíhání. Během testování bylo zjištěno, že SQL injection v základní konfiguraci je nastavený jako útok z vnější sítě. Pro detekci SQL injection z vnitřní sítě bylo potřeba vytvoření speciální sady pravidel kontrolující vnitřní síť. Logickou úvahou jak obejít bezpečnostní systém bylo experimentováno s přenosem šifrované komunikace. Tato úvaha byla potvrzena a důkladným testováním bylo zjištěno, že IDS/IPS, realizováno nástrojem Snort, není schopný detekovat šifrovaný přenos informací. Jako ověření této skutečnosti bylo využito více metod. Například využitím přenosu HTTPS nebo pomocí OpenVPN vytvoření šifrovaného tunelu mezi dvěma počítači. Prostřednictvím tohoto tunelu byly zpětně využity předchozí detekované počítačové útoky, tentokrát bez odezvy IDS/IPS a tím byl splněn hlavní cíl bakalářské práce.

Vedlejším cílem bakalářské práce bylo navrhnout, na základě testování, optimální nasazení IDS/IPS v síti. Kromě ideálního umístění v síti práce obsahuje i konfigurační návrh a upozornění na aktivní činnost IPS. Dále také upozornění na finanční náročnost tohoto bezpečnostního systému a návrh, jak lze případně finanční náklady redukovat.

Seznam literatury

[1] Monitoring sítě - jaké jsou základní kameny. *ICT Security* [online]. Nezávislý odborný on-line magazín, 2010. [cit. 9.12.2013]. Dostupné z: http://www.ictsecurity.cz/09/06/2-monitoring-site/monitoring-site-jake-jsou-zakladni-kameny.html

[2] CHAPMAN, D. Brent a ZWICKY, D. Elizabeth. *Firewally.* Principy budování a udržování. Praha: Computer Press, 1998. 508 s. Edice: PROFI pro odborníky. ISBN 80-7226-051-0

[3] Softwarové firewally. *Antivirové Centrum* [online]. Firewally, 1998-2013. [cit. 9.12.2013]. Dostupné z: http://www.antivirovecentrum.cz/firewally.aspx

[4] FROUZOVÁ, Adriana. Firewally [online]. Firewally, 2011. [cit. 9.12.2013]. Dostupné z: http://home.zcu.cz/~afrouzov

[5] ROITER, Neil. Nová generace firewallů. *Security World*. 2.12.2011, č.3, str. 5. ISSN 1802-4505.

[6] SCAMBRAY, Joel a McCLURE, Stuart a KURTZ, *George. Hacking bez tajemství.* 2. aktualizované vydání. Praha: Computer Press, 2002. ISBN 80-7226-644-6

[7] HORÁK, Michal. Jak mohou pomoci systémy detekce a prevence narušení. *IT Systems* [online]. 2005, č.11, str. 64-66. [cit. 9.12.2013]. Dostupné z: http://www.actinet.cz/pdf/ccbs-acti-clv-0512.pdf

[8] KUAN, Chia Chee. Systém IPS pro sítě Wi-Fi. *Security World*. 9.3.2012, č.1, str. 37. ISSN 1802-4505

[9] Bc. HEJTMAN, Jan. *Získávání dat z cizího počítače a možnosti aktivní obrany*. Zlín, 2010. Diplomová práce. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky.

[10] GRYGAR, Josef. *Detekce a prevence počítačového útoku*. Zlín, 2007. Diplomová práce. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky.

[11] PŘIBYL, Tomáš. Zákeřný útok jménem DoS. *IT Systems*. 11/2006, str. 56. ISSN 1802-615X

[12] ČÍŽEK, Zdeněk. Snort jakoopen sourceetalon pro IPS. *Security World*. 13.3.2009, č.1, str. 23. ISSN 1210-9924

[13] Secure Sockets Layer. *Wikipedia.org* [online]. Secure Sockets Layer, 2.9.2013. [cit. 9.12.2013]. Dostupné z: https://cs.wikipedia.org/wiki/Secure_Sockets_Layer

[14] Manual. *Snort.org* [online]. Writing Snort Rule, 2003-2013. [cit. 9.12.2013]. http://manual.snort.org/node27.html

[15] Nmap Network Scanning. *Nmap.org* [online]. Port Scanning Techniques, 2013. [cit. 9.12.2013]. Dostupné z: http://nmap.org/book/man-port-scanning-techniques.html

Seznam obrázků

OBRÁZEK 1 - BEZPEČNOSTNÍ STRUKTURA VNITŘNÍ SÍTĚ 3
OBRÁZEK 2 - FIREWALL 4
OBRÁZEK 3 - UMÍSTĚNÍ IDS V SÍTI 7
OBRÁZEK 4 - HOST-BASED VS. NETWORK-BASED 10
OBRÁZEK 5 - SNORT KOMPONENTY 13
OBRÁZEK 6 - STRUKTURA SNORT PRAVIDLA [VLASTNÍ ZDROJ] 15
OBRÁZEK 7 - SNORTEM VYDANÁ VÝSTRAHA 16
OBRÁZEK 8 - OBECNÝ POSTUP ÚTOKU 18
OBRÁZEK 9 - DDOS ÚTOK 22
OBRÁZEK 10 - SCHÉMA ZAPOJENÍ[VLASTNÍ ZDROJ] 24
OBRÁZEK 11 - MIRROR PORT 26
OBRÁZEK 12 - VLASTNÍ WEBAPLIKACE [VLASTNÍ ZDROJ] 33
OBRÁZEK 13 - PŘEHLED ZÍSKANÝCH VÝSLEDKŮ[VLASTNÍ ZDROJ] 37

Příloha 1 - Konfigurace Snort

Stažení a instalace potřebných komponent (vyžaduje registraci)

Snort (version 2_9_5_5) - http://www.Snort.org/Snort-downloads?

Snort pravidla (version 2955) - http://www.Snort.org/Snort-rules/?

WinPcap (version 4.1.3) - http://www.winpcap.org/install/default.htm

Notepad ++ (version 6.5.1) - http://notepad-plus-plus.org/download/v6.5.1.html

Po instalaci jednotlivých komponent je potřeba lokální konfigurace Snortu (Snort.conf) vždy pomocí Notepad ++, který je na dané operace nejoptimálnějším nástrojem.

Nastavení lokální IP adresy

```
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.2.0/24
```

Definice cesty k pravidlům Snortu

```
var RULE_PATH c:\snort\rules
var SO_RULE_PATH c:\snort\so_rules
var PREPROC_RULE_PATH c:\snort\preproc_rules
```

Definice cesty k porovnávacím knihovnám

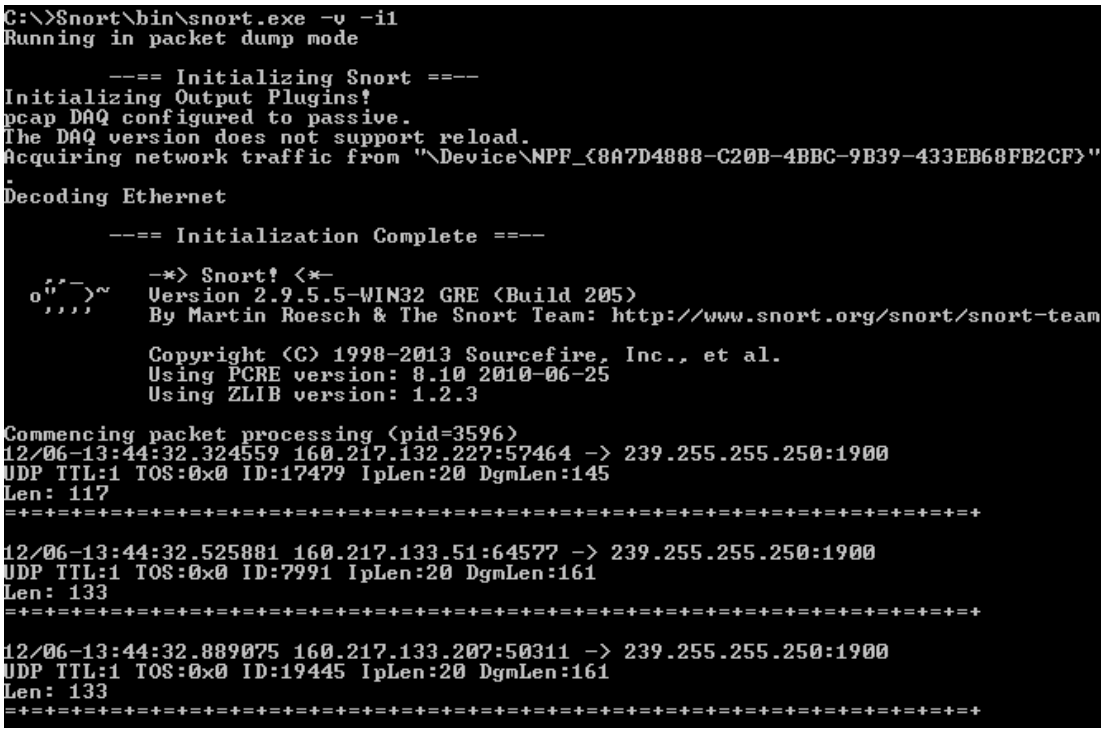
```
# path to dynamic preprocessor libraries
dynamicpreprocessor directory c:\snort\lib
\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine c:\snort\lib\snort_dynamicengine\sf_engine.dll

# path to dynamic rules libraries
#dynamicdetection directory c:\snort\lib\snort_dynamicrules
```

Definice výstupních výstrah (do souboru alerts.ids)

```
# pcap
# output log_tcpdump: tcpdump.log
output alert_fast: alerts.ids
```

Přes příkazový řádek spuštění Snortu a zjištění, jaký interface použít pro odchytávání paketů

Spuštění Snortu v režimu sniffer (příkaz -v -i a číslo interfacu)



Spuštění Snortu v režimu NIDS

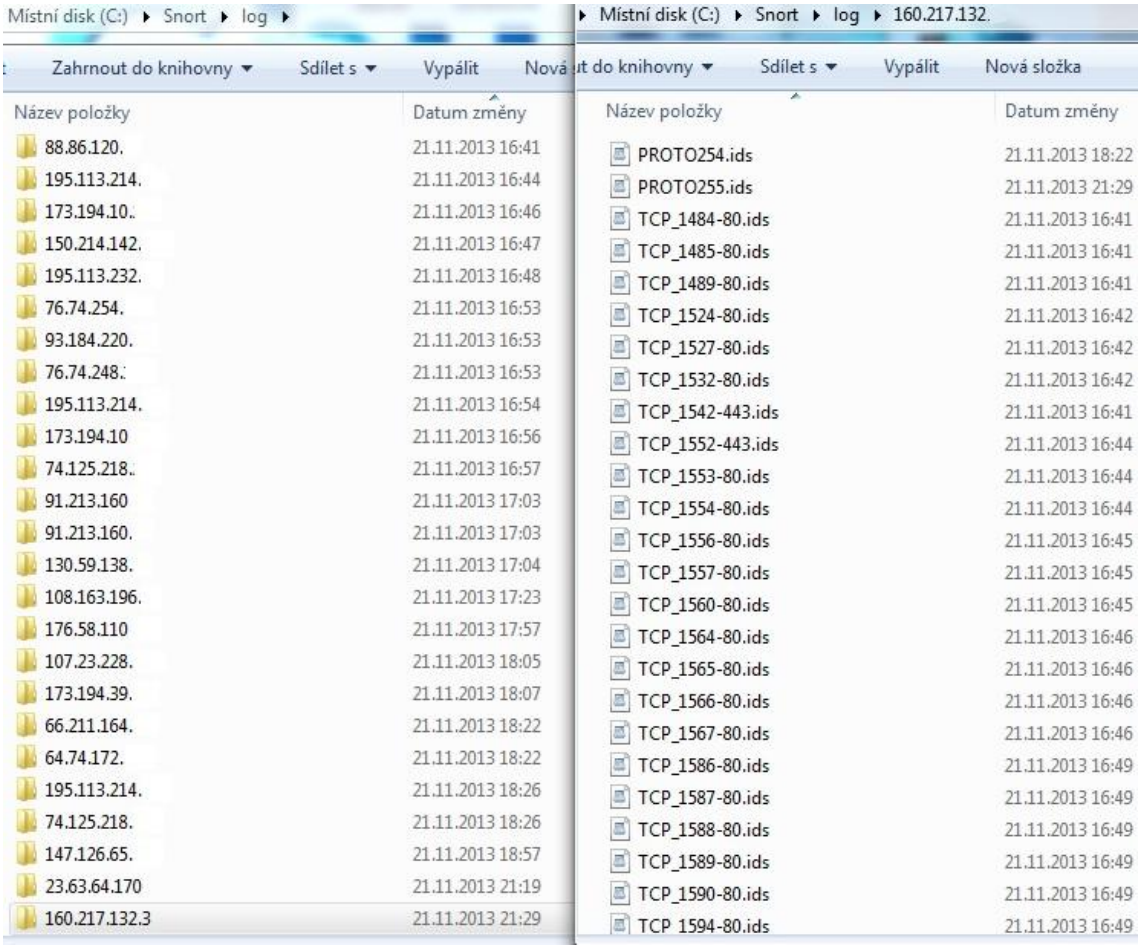
Snort.exe -A console -i1 -c c:\Snort\etc\Snort.conf -l c:\Snort\log -K ascii

Jelikož je spuštění Snortu v NIDS poměrně dlouhý příkaz a během testování je nutné upravovat pravidla a znovu načítat pomocí tohoto příkazu, byl vytvořen skript (ids.bat).

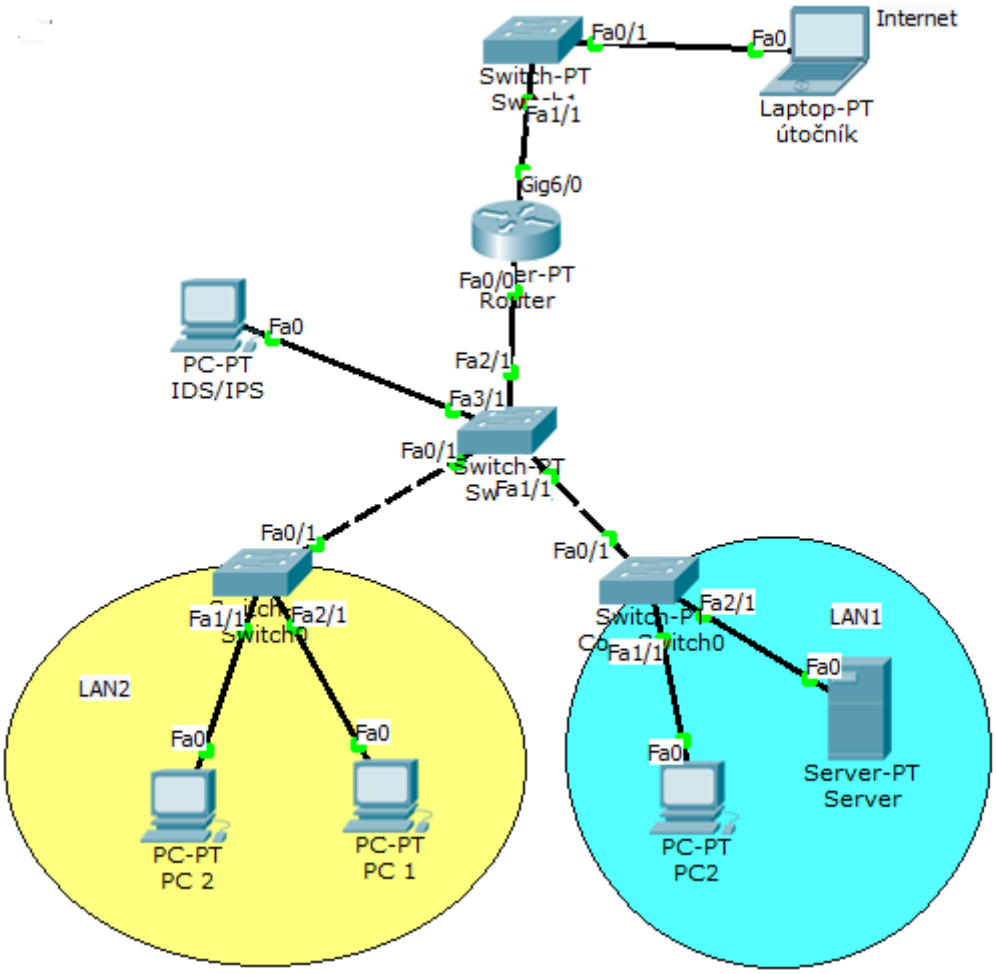
```
cd\
cd snort\bin
cls
@ echo Running Snort IDS System Setup by David
snort -A console -i1  -c c:\snort\etc\snort.conf -l c:\snort\log -K ascii
```

Ukázka konfigurace jsou pouze základním uvedením Snortu do provozu. V průběhu používání a testování bylo potřeba dalších úprav a rozšiřujících konfigurací.

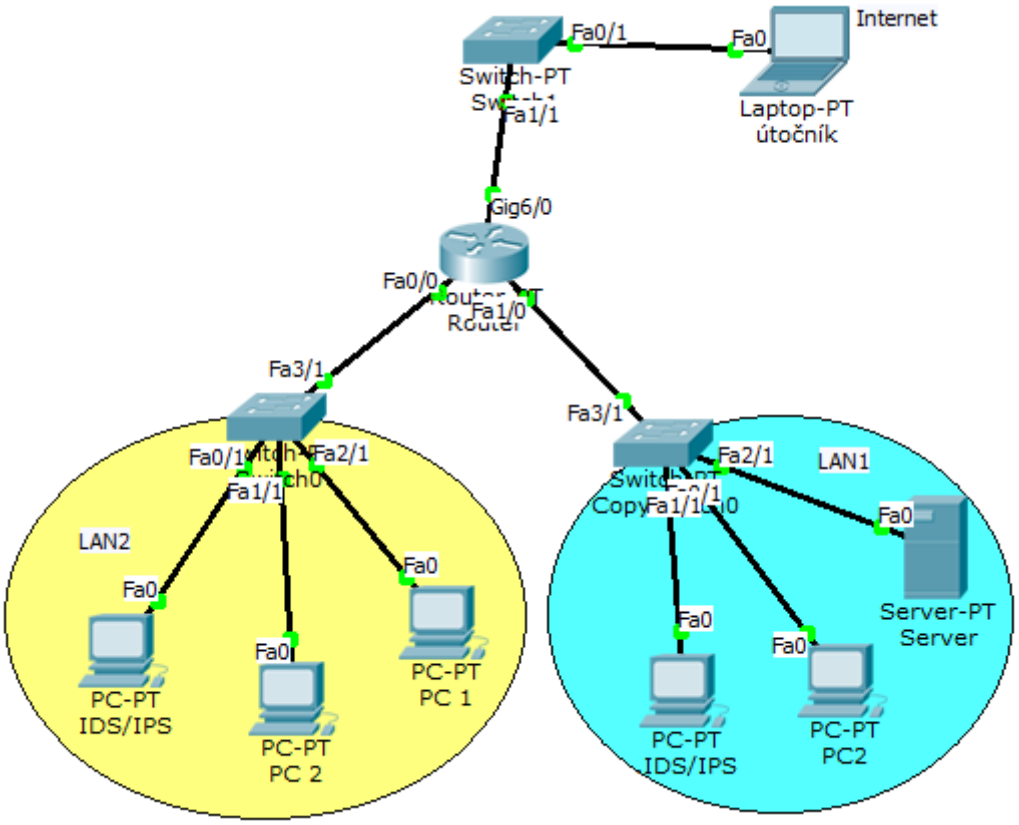
Příloha 2 - Ukázka logu s výstrahami detekovanými během jednoho dne běžného využití internetu z jednoho PC. Z důvodu osobního soukromí jsou poslední číslice IP adresy skryty.



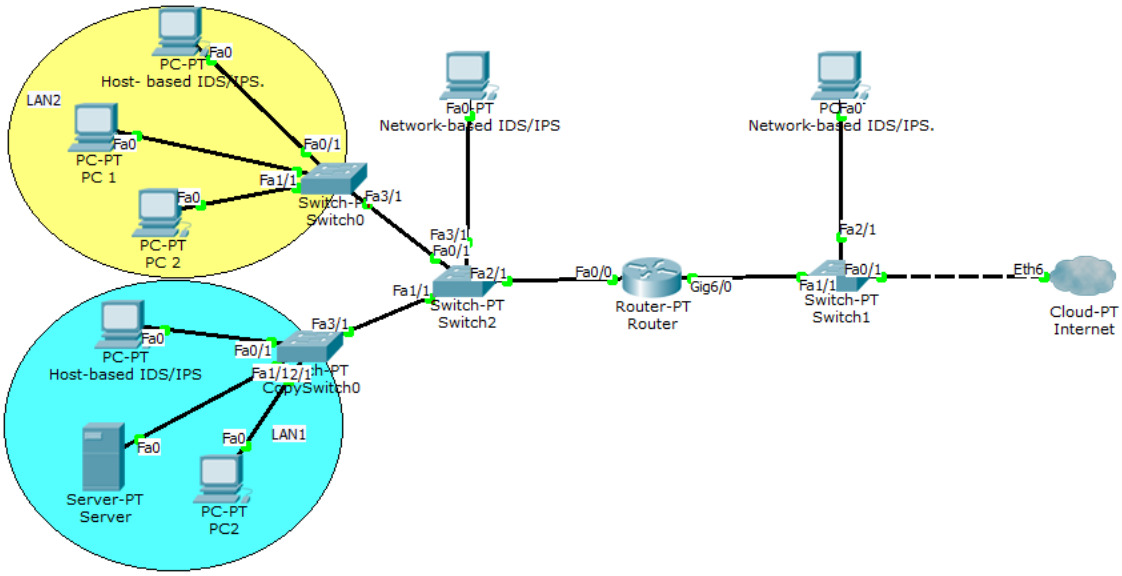
Příloha 3 - Optimální nasazení IDS/IPS za předpokladu, že je síťová topologie rozdělena na několik VLAN a všechny musí být analyzovány jedním systémem.



Příloha 4 - Optimální nasazení IDS/IPS, pokud je možné využít více bezpečnostních systémů.



Příloha 5 - Návrh optimálního nasazení IDS/IPS.



Přílohy - další části přiložené k práci

[1] CD s bakalářskou prací (včetně příloh) v elektronické podobě.