Intrusion Detection System

Jiří Maršíček

Abstrakt **– Text uvádí do problematiky Intrusion Detection Systémů. V první části s těmito systémy seznamuje obecně. Druhá část je pak věnována konkrétní implementaci – softwaru Snort, jeho instalaci a základní funkcionalitě.**

1. Úvod

V dnešní době je bezpečnost informačních systému tak důležitá, že už nestačí jednoduché prevence proti útokům a možným vniknutím.

Bežný firewall nedokáže detekovat a zábránit síťovému provozu, který, ač je podle politik firewallu naprosto korektní, může být počátkem záludného útoku do naší sítě. K detekování takových síťových anomálií a útoků slouží Intrusion detection system.

1.1. Definice

Jak již z názvu vypovídá, primárním účelem Indtrusion Detection Systému (dále jen IDS) je odhalování průniků do počítačových sítí. Zjištění takových informací je klíčem k tomu, abychom se dozvěděli jakými způsoby je do sítě pronikáno. Takové znalosti nám mohou pomoci v lepším zapezpečení sítě.

1.2. Druhy IDS

Nejvíce rozšířeným IDS je tzv. Network Intrusion Detection System nebo-li NIDS. Takový systém je připojen do určitého segmentu sítě (v případě malé sítě se může jednat o celou síť) a naslouchá veškerému provozu.

Zpravidla v síti nacházíme více NIDS najednou – tyto nazýváme senzory - v různých segmentech. Získaná data jsou pak posílána ihned nebo periodicky na server, který je uchovává například v relační databázi. [2]

Dalším druhem IDS je tzv. Host-based Intrusion Detection System nebo-li HIDS. Takový systém je na každém síťovém zařízení, u kterého chceme mít informace o síťových anomáliích, které nebývají běžně zaznamenané.

HoneyPot nebo-li česky sklenička medu je specifickým druhem IDS. V síti je lákadlem pro škůdce, kteří jsou zlákáni slabou obranou takového systému. Je přitom žádoucí, aby byl nakonfigurován jako plnohodnotný systém, aby iluze byla co nejpřesvědčivější. Získání dat o tom jak útočník do sytému pronikl a jak si v něm počínal je hlavním úkolem HoneyPotů. [3]

Na závěr je nutné zmínit ještě tzv. Intrusion Prevention System nebo-li IPS. Takový systém v sobě integruje IDS, k tomu aby získal informace o probíhajícím útoku v síti, a zároveň nástroje, které dokáží tento útok přerušit a případně před ním i do budoucna chránit.

Nadále se budeme zabývat jen NIDS implementací, která se dá celkem úspěšně brát jako zobecněná verze ostatních.

2. Nasazení IDS

2.1. Kdy a k čemu je IDS dobrý

Nasazení prostředku jakým je IDS je užitečné pouze tehdy, dokážeme-li získané informace vyhodnocovat a dále s nimi pracovat.

Dokáže zaznamenávat síťovou aktivitu z vnitřního perimetru sítě, který je často považovaný za bezpečný, ovšem z praxe vyplívá, že nejvíce útoků je vedeno právě odsud. Jestliže tedy takové nekalosti chceme mít pod kontrolou je dobré nasazení takového systému zvážit.

2.2. Kam IDS v síti umístit

Aby měl IDS nějáký význam, je nutné, aby naslouchal veškerému provozu na síti. V sítích s huby toto není problém. Ve switchovaných sítích je u switchů vyžadována možnost nastavení posílání veškerého provozu na jeden port - pro tento port se switch jeví jako hub.

IDS se nejčastěji umísťuje za firewall nebo za router, dělící lokální síť od sítě Internet. V případě složitějších sítí je nutné umístit senzor IDS v každém segmentu sítě, případně jen v částech, které chceme monitorovat.

2.3. Výběr produktu

Nejznámějším produktem na poli open source software je Snort od firmy Sourcefire. Tento software je vydán pod licencí GNU. [4] Je mu věnována následující kapitola.

Firma Sourcefire vyvýjí a nabízí i pokročilejší a sofistikovanější produkty IDS pro enterprise nasazení. Tyto produkty už ale nejsou vydávány pod GNU licencí, ale jejich pořízení je zpoplatněno.

Podíl firmy Sourcefire v open source komunitě je nicméně nepřehlédnutelný, vedle Snortu vlastní i známý antivirový software ClamAV. [4]

Snort není jediný hráč na poli open source IDS. Jedním z dalších je Bro IDS vydanný pod BSD licencí, který je cílený na gigabitové sítě s velkým přenosem dat. [5]

Zároveň existují i další komerční řešení. Například od firmy Cisco a její produkty Cisco IDS a IPS. [6] Dále produkty z této sféry nabízí firma CheckPoint s její řadou kompletních řešení IPS a SmartDefense. [7] Není to konečný výčet všech dostupných systémů.

Z kategorie Honeypot softwaru zmíním např. LaBrea, který je používaný v síti ČVUT. [8] Dobrým výchozím bodem pro zájemce o tuto problematiku je Honeynet Project. [9]

3. Snort

Dále se budu zabývat již konkrétním IDS, tím je Snort od společnosti Sourcefire. Úvodem se stručně zmíním o architektře systému a v další části o jeho konkrétní instalaci v systému Gentoo Linux.

3.1. Architektura

Snort může pracovat v různých módech. [1] Prvním je tzv. Network Sniffer Mode. V tomto módu Snort pouze zobrazuje zaznamenané packety na standartní výstup.

Dalším je Packet Logger Mode. V tomto módu Snort zaznamenává do logu nebo databáze všechny packety na síti. Provoz v tomto módu je datově i výpočetně velmi náročný. Pro tento mód není potřeba žádná konfigurace. Jeho možnosti jsou tedy omezené a nebudu se jím dále zabývat.

Nejzajímavějším módem je Network Intrusion Detection Mode. V tomto módu Snort nezaznamenává informace o všech packetech. Zaznamenává jen ty, které odpovídaly nějakému nakonfigurovanému pravidlu.

Pravidla mohou obsahovat informace o input nebo output plug-inech, které mohou ovlivňovat zpracování packetu a reakcí na něj. [2]

3.1.1 Základní komponenty

Snort je rozdělen do několika komponent, které v průběhu zpracování packetu hrají důležitou roli. Schématicky je toto rozdělení na *Obr. 1*.

Packet Decoder naslouchá na interfacech a připravuje packety pro další zpracování preprocesory nebo detection enginem.

Preprocessors je skupina komponent, které přijatý packet nejdříve předpřipraví k tomu, aby z něj bylo možné nějáké informace vyčíst. Sem patří například zpracování fragmentovaných packetů. Sledování TCP a UDP streamů. Preprocessorů je se Snortem dodaná celá řada, většinou mají na starosti určité protokoly a hledají anomálie na úrovni těchto protokolů (SSH, SMTP, DNS a další). [2]

Detection Engine je místo, kde se v největší míře uplatňují pravidla v konfiguračním souboru. Pravidla jsou načtena do vnitřních struktur programu a proti nim jsou porovnávány přijaté packety. [2] Zde dochází k největší zátěži a je nutné vzít v potaz výkon stroje, předpokládané vytížení sítě a počet definovaných pravidel. [1]

Logging and Alerting System se stará o to, že v případě pozitivní shody s některým pravidlem dochází k zaznamenání této informace do logu nebo vygenerování poplachu.

Output Modules je množina rozšíření, které když jsou spuštěny mohou iniciovat různé události. Příkladem je logování do databáze, posílání SNMP zpráv, generování XML výstupu nebo úprava konfigurace firewallu. [1]

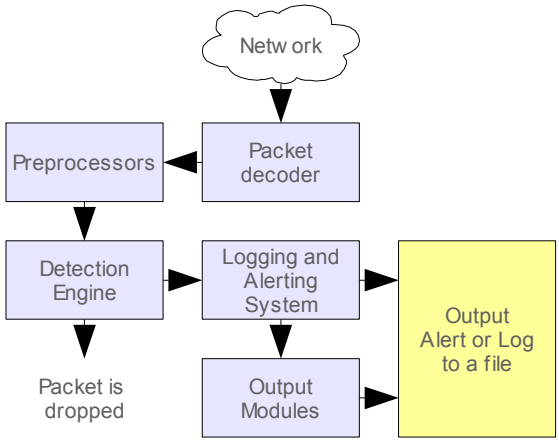
3.2. Ochrana IDS

Zajímavou kapitolou při plánování a nasazování IDS je zabezpečení samotného systému, na kterém je IDS spuštěný. Je nutné tento systém chránit, aby útočník nemohl kompromitovat zaznamenané aktivity. Pokud plánujeme provoz Snortu na Linuxu je vhodné zablokovat veškerý příchozí provoz pomocí iptables, Snort i přes toto omezení bude schopen vyhodnocovat všechny aktivity. [1]

Dalším stupněm ochrany může být naslouchání na interfacu, který má zapnutou podporu TCP/IP, ale nemá přidělenou IP adresu. Nemůže být tedy adresován a riziko napadení stroje se snižuje. Snort je i přes to schopen síťový provoz vyhodnocovat. [10]

Pro komunikaci Sensoru s databázovým serverem, případně kvůli údržbě, je vhodné takový systém vybavit dalším síťovým interfacem. Tento interface může být připojen do uzavřeného segmentu sítě, nebo do k tomu účelu vytvořené VLAN.

Nejvíce extrémním řešením je tzv. Stealth interface. Spočívá v připojení systému do monitorované sítě za pomocí "recieve-only" kabelu, kde nejsou vůbec připojené kabely pro odesílání. V kombinaci s předchozí metodou je nejbezpečnějším řešením. [10]



Obr. 1: Schéma rozdělení komponent a průběh zpracování. Převzato z [2]

3.3. Instalace v Gentoo Linux

Pro instalaci systému Snort jsem zvolil Gentoo - distribuci operačního systému Linux. Snort se nachází v Portage - podporované kolekci software. Při přípravě této práce jsem měl k dispozici Snort verze 2.8.4.1. Instaluje se pro Gentoo typickým příkazem **emerge snort**.

Následující konfigurace není nikterak složitá a nevyužívá ani zlomku možností, které Snort nabízí. Zabývá se pouze konfigurací Detection Enginu a tedy příslušných pravidel. Možnosti Output modulů jsou nad rámec této práce.

3.3.1 Nejdůležitější nastavení

K čerstvě nainstalovanému Snortu je dodaný výborně okomentovaný ukázkový konfigurační soubor **snort.conf.distrib**. Tento soubor je skvělým startovním bodem pro začínající uživatele. Výchozím názvem souboru s konfigurací je snort.conf.

Konfigurační soubor je při té nejednodušší konfiguraci souborem pravidel. O jejich tvorbě se zmiňuji v další části.

Nabízí možnost nastavení proměnných systému, mezi které může patřit síťový rozsah lokální sítě, adresy serverů nebo stanic, které jsou použity v pravidlech. Změna adresace sítě a přepis proměnných potom nebude takovým problémem jako přepisování všech pravidel.

Základní konfigurační soubor má možnost nalinkování dalších podružných souborů, tato užitečná funkce je nezbytná, když globálně spravujeme konfiguraci pro více IDS nebo automaticky aktualizujeme pravidla z internetu. Více o tom v 3.3.3.

Za zmínku stojí i soubor pro konfiguraci init skriptu, který je umístěný v tradiční cestě **/etc/conf.d/snort**. Zde lze volit cestu ke konfiguračnímu souboru, interface, na kterém má Snort naslouchat a jiné podrobnosti.

3.3.2 Úvod do tvorby pravidel

Snort používá poměrně intuitivní syntaxi psaní pravidel. Většina pravidel je napsána na jediné řádce, od verze 1.8 ovšem podporuje i pravidla víceřádková. To že pravidlo pokračuje na dalším řádku je vyznačeno znakem "/".

Pravidlo je rozděleno na dvě části: headers a options (hlavička a volby). Na *Obr. 2* je příklad jednoduchého pravidla.

```
alert tcp any any -> 192.168.1.0/24 any
(sid:1000001; flags:A; ack: 0; msg: "TCP
Ping detected";)
```

Obr. 2: Pravidlo detekující tzv. TCP ping. Převzato z [1].

Hlavička obsahuje akci, která se má provést. Zde je to "alert", tedy vygenerování poplachu a zalogování packetu.

Dále je zde protokol, kterého se pravidlo týká – zde "tcp". Následuje zdrojová adresa a maska a zdrojový port. Hodnota "any" značí že se aplikuje na všechny hodnoty.

Šipka znázorňuje směr komunikace, možnosti jsou: "->" pro komunikace od zdroje k cíli, "<>" pro koumunikaci v obou směrech a "<-" pro komunikace od cíle ke zdroji.

Následuje cílová adresa a maska a cílový port.

Volby jsou uvedeny v závorce. Zatímco hlavička má formát předepsaný a všechny položky jsou povinné, volby nemusí být uvedené vůbec. Voleb je velké množství a pro detailní informace o všech odkazuji na oficiální dokumentaci.

```
[**] [1:1000001:0] TCP Ping detected [**]
[Priority: 0]
05/24-14:41:06.453957 192.168.1.5:48118 -> 192.168.1.4:22
TCP TTL:64 TOS:0x10 ID:35993 IpLen:20 DgmLen:52 DF
***A**** Seq: 0x0  Ack: 0x0  Win: 0x1F5  TcpLen: 32
```

Obr. 3: Záznam packetu, který odpovídal pravidlu z Obr. 2.

Volba Sid jednoznačně identifikuje pravidlo číslem. Volba Flags říká jaký příznak musí mít packet, aby na něj bylo pravidlo aplikováno. Zde "A" jako ACK. Volba Ack říká jaké číslo potvrzení musí packet mít, aby na něj bylo pravidlo aplikováno. Volbou "Msg" přidáváme dodatečné informace, které se zapíší do logu.

Záznam v logu, který packet odpovídající pravidlu z *Obr. 2.* je vidět na *Obr. 3*.

3.3.3 Zdroje pravidel

Způsobů jak provést průnik do sítě je nepřeberné množství, není tedy v silách jednotlivce obsáhnout všechny tyto znalosti a vytvářet všechna pravidla konfigurace. Existují proto zdroje celých souborů pravidel dostupných ke stažení z Internetu.

Sourcefire VRT Certified Rules je soubor pravidel dodávaný firmou, která má vývoj Snortu na starosti. [11] Pravidla jsou periodicky upravována a jsou dostupná k bezplatnému stažení registrovaným uživatelům. Uživatelům, kteří si za registraci zaplatí jsou k dispozici častější updaty a novější verze.

Emerging Threats je projekt spravovaný open source komunitou. [12] Dostupnost pravidel není zpoplatněna ani není podmíněna registrací a nejnovější verze je dostupná všem. Nové verze jsou vydávány týdně.

Na závěr nemohu opomenout projekt nazvaný Oinkmaster. [13] Je to skript, který slouží k správě a updatu pravidel. Je to výborný nástroj pro centralizovanou správu více senzorů, ale i pro bezúdržbový provoz jediného. Projekt je vydaný pod BSD licencí.

Oinkmaster je dostupný v Gentoo Portage a nainstaluje se příkazem **emerge oinkmaster**.

3.4. SnortSam

SnortSam je doplněk Snortu, který má na starosti úpravu pravidel firewallu. S tímto rozšířením se ze Snortu a podporovaného firewallu může stát plnohodnotny Intrusion Prevention System.

Skládá se z Output Modulu na straně IDS a z agenta na straně firewallu. Podporuje celou škálu různých implementací firewallu na různých platformách. Pro nás je důležitá podpora Linux Iptables.

Komunikace agenta se senzorem IDS je šifrovaná. V případě, že dojde k události, na kterou má modul reagovat, odešle upozornění agentům a oni upraví konfiguraci svých firewallů.

SnortSam je také součástí Gentoo Portage a nainstalovat jej lze příkazem **emerge snortsam**. Jak Snort spolu se SnortSam plug-inem nakonfigurovat je popsáno na oficiální stránce projektu. [14] Pro základní konfiguraci doporučuji prostudovat "Creating a Intrusion Prevention System (IPS) using Snort and SnortSam" na webu uno-code.com. [15]

4. Závěr

Během vytváření tohoto dokumentu jsem dosáhl svého cíle seznámit se se základy systému Snort. Zkusil jsem si konfiguraci jednoduchých pravidel i načtení pravidel z veřejných zdrojů. Nejvíce mě ovšem zaujala kombinace systému Snort s rozšířením SnortSam. Dohromady tvoří výbornou dvojici v obraně proti sofistikovaným útokům.

Zájemce o tuto problematiku odkazuji na seznam zdrojů a zvláště doporučuji knihu **Intrusion Detection Systems with Snort** od Rageeqa Ur Rehmana, která je volně dostupná ke stažení.

Reference

Seřazené podle výskytu v textu.

[1] Intrusion Detection Systems with Snort, Rafeeq Ur Rehman, ISBN 0-13-140733-3

[2] http://www.snort.org/docs/snort_htmanuals/htmanual_284/ , 2009-05-26

[3] http://en.wikipedia.org/wiki/Honeypot_(computing) , 2009-05-26

[4] www.sourcefire.com/company/ , 2009-05-26

[5] www.bo-ids.org/ , 2009-05-26

[6] http://www.cisco.com/en/US/products/sw/secursw/ps2113/index.html , 2009-05-26

[7] http://www.checkpoint.com/products/intrusion-prevention-systems.html , 2009-05-26

[8] http://labrea.sourceforge.net/labrea-info.html , 2009-05-26

[9] http://www.honeynet.org/ , 2009-05-26

[10] http://www.snort.org/docs/faq/3Q06/ , 2009-05-26

[11] http://www.snort.org/pub-bin/downloads.cgi , 2009-05-26

[12] http://www.emergingthreats.net/ , 2009-05-26

[13] http://oinkmaster.sourceforge.net/ , 2009-05-26

[14] http://www.snortsam.net/ , 2009-05-26

[15] http://www.uno-code.com/?q=node/59 , 2009-05-26