Monitorovací síťový systém SAVO

Monitoring network system SAVO

Martin Papík[1,2], Milan Zajíček[2], Petr Vaníček[2]

[1]Katedra informačního inženýrství, PEF, Česká zemědělská univerzita v Praze, Kamýcká 129, 165 21 Praha 6
[2]Ústav teorie informace a automatizace AVČR, v.v.i., Pod Vodárenskou věži 4, 182 08 Praha 8
papik@pef.czu.cz

Anotace. Cílem projektu je získat automaticky fungující systém výstrahy sledující kybernetické útoky s původem v adresním prostoru Akademie věd České Republiky SAVO (Secure AV Outbound). Informace získané analýzou provozu mezi sítí AV ČR a nástražným systémem umožní informovat zodpovědná pracoviště o potenciálním nebezpečí.

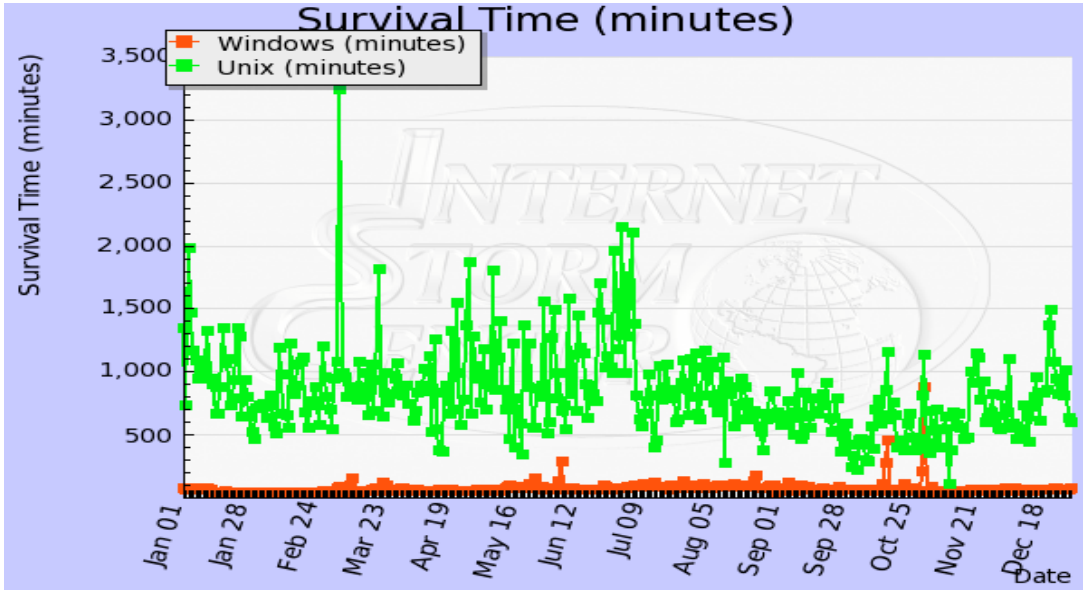
Klíčová slova: IDS, Firewall, Honeypod

Annotation. Target of this project is creating of the functional alert system for network attacks named SAVO (Secure AV Outbound). This system is dedicated for AV (Academy of Sciences of the Czech republic) network. Informations which obtained from monitoring (analysis) will be aviable for responsible ICT departments.

Key words: IDS, Firewall, Honeypod

1 Úvod

Časy, kdy bylo možné ponechat v Internetu „nezáplatovaný“ počítač bez dozoru i po několik měsíců, aniž by doznal závažnější újmy, jsou nenávratně pryč. S masivním rozšířením automaticky se propagujících červů je současná životnost implicitních instalací běžných operačních systémů (Windows, Linux) velmi nízká, u některých se pohybuje pouze v desítkách minut, podle [6]. Následující graf č.1 ukazuje statistiku životnosti operačních systémů v minutách (osa *y*), přičemž se jedná údaje za celý rok 2007.



Graf 1. Životnost implicitních instalací operačních systémů, podle [6].

2 Cíl

V polovině roku 2008 se rozběhl projekt SAVO (Secure AV Outbound), který je realizován několika pracovišti AVČR. Tento projekt si klade za cíl vybudovat systém pro detekci útoků uvnitř akademické sítě PASNET (Pražská akademická síť), resp. jejího segmentu který používá AVČR. V rámci tohoto projektu budou použity moderní technologie (zařízení a software) pro detekci a vyhodnocení útoků, například systém pro detekci průniku - IDS (Intrusion detection system), návnadné systémy (tzv. Honeypod) a systémy pro vizualizaci dat. Projekt SAVO by měl mít i zpětnou informační vazbu směrem na správce jednotlivých sítí, pokud bude zjištěn útok přicházející z dané sítě.

Prezentace výsledků provozu tohoto systému by měla proběhnout na jaře 2009.

3 Způsob řešení

Centrálním uzlem systému je firewall (Juniper ISG1000) od letošního roku doplněný o IDS systém umožňující monitorování nejrůznějších druhů kybernetických útoků. Informace o druhu, četnosti a závažnosti útoků lze získat pomocí systému NSM (Netscreen security manager), sloužícího pro vzdálenou správu firewallů Juniper. Tento systém rovněž umožňuje získat strukturovaný soubor, který bude sloužit jako množina dat, jejímž filtrováním a analýzou získáme informaci o napadených systémech ze sledovaných sítí, na které systém SAVO upozorní (nejlépe e-mailem) správce dotčených uzlů.

Pro správnou funkci systému je třeba návnadný systém, který je tvořen nejrůznějšími službami a jejich otevřenými porty (služby MS Windows, databázové služby, webové služby atd.) V praxi bude vytvořen jako oddělený segment sítě s jedním počítačem (serverem), na kterém bude formou virtuálních zařízení provozováno několik systémů obsluhujících výše uvedené služby.

Samotná implementace návnadného systému je provedena metodou "Honeypot", což je počítač, který emuluje uzel sítě i s jeho službami a umožňuje sledovat aktivity útočníka. Jako typický příklad lze uvést například program honeyd [8]. Tento software umožňuje na jediném počítači implementovat celé sítě virtuálních zařízení, která se tváří tak, jako by provozovala rozličné operační systémy a služby. Umožňuje rovněž simulovat různé síťové topologie se směrovači, latencí a simulovanými ztrátami paketů.

Běžné konfigurace honeyd se hodí k detekci pokusů o útoky. Nedokáží však zachytit celý průběh útoku anebo škodlivý kód červa. K tomu je uzpůsoben systém NEPENTHES [9]. Ten dokáže emulovat známé bezpečnostní díry, díky kterým se červi šíří, a z analýzy síťového provozu pak získat informaci o původci a způsobu útoku.

Poněkud jiný přístup k detekci a analýze útoků a škodlivého kódu představuje projekt DARKNET [1]. DarkNetem se rozumí část alokovaného a běžně směrovaného IP prostoru, ve kterém se nenachází žádný aktivní server nebo služba. Z hlediska uživatele je taková síť zcela prázdná. Ve skutečnosti ale obsahuje alespoň jeden server, který zachytává a analyzuje veškerý provoz, který se v „DarkNetu“ objeví. Jelikož v něm neběží žádná uživatelská služba, může být provoz způsobený pouze chybnou konfigurací některého zařízení na síti, anebo je jeho původcem nekalá aktivita.

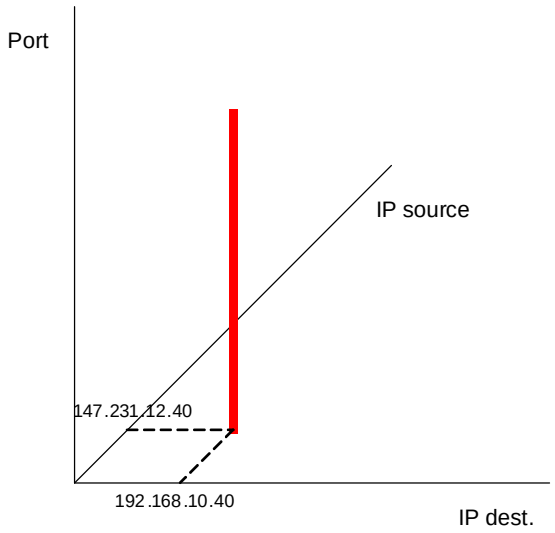
Vzhledem k tomu, že výstražné informace z IDS mohou obsahovat množství falešných poplachů (např. informační email s popisem útoku může být vyhodnocen jako falešný útok),

pokusíme se kombinací informací z honeypotů (případně „DarkNetu“) a IDS omezit jejich výskyt a zvýšit tak relevantní použitelnost celého systému na co nejvyšší míru.

Pro analýzu a monitorování potenciálně škodlivého provozu bude použit některý z obvyklých nástrojů, například Snort či Wireshark.

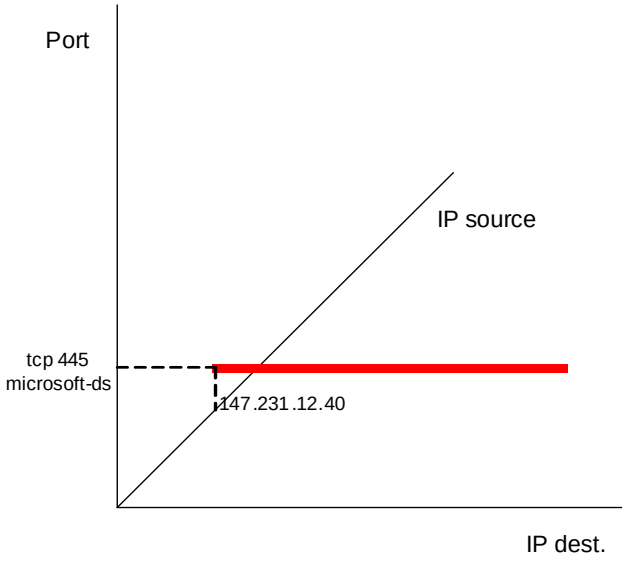
4 Grafická reprezentace síťového provozu – vizualizace dat

V podstatě se jedná o grafické zobrazení ve 2D či 3D prostoru. Kdy lze lehce rozpoznat skenování portů, útok červa nebo i útok na počítač (server) o který je všeobecný zájem (DDOS útok). Na následujícím obrázku č.1 je znázorněno skenování portů, kdy osa *x* odpovídá IP adresám monitorované sítě (destination IP), osa *z* odpovídá IP adresám externí sítě (source IP) a osa *y* odpovídá cílovým portům.



Obr. 1. Skenování portů

Další obrázek č. 2 znázorňuje DDOS (Distributed denial of service) útok.



Obr. 2. DDOS útok

Jde o zajímavou myšlenku, která byla dotažena do konce, například v podobě softwarového nástroje Rumint [6] nebo Cube of Potential Doom [7].

Tyto nové postupy pro „vizuální“ analýzu budou také využívány v rámci projektu SAVO.

5 Závěr

Všechny zmíněné nástroje a postupy lze využít k detekci a analýze útoků. Projekt SAVO se bude snažit tyto prostředky vhodně kombinovat tak, aby relevance získaných informací byla co největší. Musíme si uvědomit, že na rozdíl od IDS jsou například nástražné systémy a programy sloužící ke grafickému znázornění dat prostředky pasivní bezpečnosti (tj. dokáži reagovat až po provedení útoku). Naproti tomu IDS je systém aktivní bezpečnosti (reaguje už v době provádění útoku). IDS jsou však velmi složité systémy po stránce administrace a při špatné konfiguraci mohou produkovat množství falešných útoků. Proto má velký smysl i pro samotné ladění konfigurace IDS použít poznatky z pasivních bezpečnostních prvků, aby prvotní nadšení z pořízení nového IDS brzo neopadlo díky nevhodné konfiguraci jeho pravidel.

Autoři pevně věří, že po určité době, která je nutná ke shromáždění statistických dat, budou moci představit konkrétní bezpečnostní poznatky a doporučení, která díky projektu SAVO získají.

Reference

1. Břehovský P. Některé méně tradiční metody detekce škodlivých aktivit v IP sítích. *Sborník XXXII. Konference EurOpen*. Plzeň 2008. ISBN 978-80-86583-14-3.
2. Jirkovský V. Kybernetická kriminalita. Praha 2007. ISBN 978-80-247-1561-2.
3. Thomas T. Zabezpečení počítačových sítí. Brno 2005. ISBN 80-251-0417-6.
4. Wiliam Ch., Steven B. Firewalls and Internet Security. Reading 1994. ISBN 0-201-63357-4
5. Cameron R. Netscreen Firewalls. Rockland 2005. ISBN 1-932266-39-9.
6. Internet Storm Center - ISC. http://isc.sans.org
7. Juniper Network, Inc. http://www.juniper.net
8. Money.org Developments. http://www.honeyd.org
9. Nepenthes. http://nepenthes.mwcollect.org
10. Rumint. http://www.rumint.org
11. GPL Cube of Potential Doom. http://kismetwireless.net/doomcube