ГОДИШНИК на Минно-геоложкия университет "Св. Иван Рилски", Том 51, Св.III, Механизация, електрификация и автоматизация на мините, 2008
ANNUAL of the University of Mining and Geology "St. Ivan Rilski", Vol. 51, Part III, Mechanization, electrification and automation in mines, 2008

СИСТЕМА ЗА АВТОМАТИЗИРАНО РАЗПОЗНАВАНЕ И ОПОВЕСТЯВАНЕ НА НЕДОБРОНАМЕРЕНИ И НЕКОРЕКТНИ ДЕЙСТВИЯ В КОМПЮТЪРНА МРЕЖА

Стефан Димитров[1], Веселин Колев[2], Веселка Спасова[3]

[1]Софийски университет "Св. Кл. Охридски", 1164-София, e-mail: stefan@ucc.uni-sofia.bg
[2]Софийски университет "Св. Кл. Охридски", 1164-София, e-mail: vlk@lcpe.uni-sofia.bg
[3]Софийски университет "Св. Кл. Охридски", 1164-София, e-mail: v_spasova@abv.bg

РЕЗЮМЕ. Все повече IT системи, приложения и услуги се публикуват в Интернет. Тяхната поява води до появата и на нови заплахи, които експлоатират все по-ефективно пропуските им в сигурността. Целта на настоящата разработка е да се предложи решение за проектирне и създадване на система за автоматизирано разпознаване и оповестяване на недобронамерени и некоректни действия в компютърна мрежа.
Предложението се базира на използване на некомерсиална система Prelude. Намерено е такова решение, чрез което IP адресите на подателите на лоши заявки се извличат от журналния файл prelude.log и да се подават на съответния мрежов филтър (IPTABLES, IPCHAINS и др.) в реално време, за да може да бъде прекъснат по най-бърз начин отговора на лошите заявки, а оттам и натоварването на изходящите линии.

SYSTEM FOR AUTOMTED INTRUSION DETECTION AND REPORTING IN COMPUTER NETWORK

Stefan Dimitrov[1], Vesselin Kolev[2], Veselka Spasova[3]
[1]Sofia University"St. Kliment Ohridski", 1164-Sofia, e-mail: stefan@ucc.uni-sofia.bg
[2]Sofia University"St. Kliment Ohridski", 1164-Sofia, e-mail: vlk@lcpe.uni-sofia.bg
[3]Sofia University"St. Kliment Ohridski", 1164-Sofia, e-mail: v_spasova@abv.bg

ABSTRACT. More and more IT systems, applications and services are published in Internet. This leads to the appearance of new threats that exploit more effectively the breaches in security. The aim of the present paper is to offer solution for a system for automated intrusion detection and reporting in computer network.
The proposal is based on open source system Prelude. Solution is found that in real time the source IP addresses of bad queries are extracted from the log file prelude.log and are entered into the corresponding network filter (IPTABLES, IPCHAINS, etc.). In this way most quickly response to bad queries is broken and overload of output lines as well.

Въведение

Все повече IT системи, приложения и услуги се публикуват в Интернет. Тяхната поява води до появата и на нови заплахи, които експлоатират все по-ефективно пропуските им в сигурността.Целта на настоящата разработка е да се предложи решение за проектирне и създадване на система за автоматизирано разпознаване и оповестяване на недобронамерени и некоректни действия в университетска мрежа [2, 3].

Предложението се базира на използване на некомерсиалната IDS система Prelude [1]. Prelude е продукт, който успешно детектира лоши заявки за определен набор от портове по протокол TCP. Предимството му е, че ако бъде инсталиран и стартиран върху маршрутизатор, той преглежда всички заявки, които преминават от вън към вътрешните мрежи. Prelude по подразбиране не взаимодейства с мрежовите филтри като IPTABLES и IPCHAINS. Т.е. този инструмент има само ролята на статист, наблюдател на заявките, които преминават.

Стратегия за решаване на проблема с лошите заявки

Тъй като самата програма Prelude само регистрира заявките, а не ги игнорира е нужно да се намери такова решение, чрез което IP адресите на подателите на лоши заявки да се извличат от журналния файл prelude.log и да се подават на съответния мрежов филтър (IPTABLES, IPCHAINS и др.) в реално време, за да може да бъде прекъснат по най-бърз начин отговора на лошите заявки, а оттам и натоварването на изходящите линии [9].

Форматът на журналния файл за всяка една лоша заявка е следния:

```
*** Wed Jan 30 14:24:20 2002 - Wed Jan
30 14:24:23 2002

Plugin : HttpMod
Author : Yoann Vandoorselaere
Contact : yoann@mandrakesoft.com
description : Snort based http decode
plugin.
kind : May not be reliable
received : 6 times
```

```
message : ISS Unicode attack detected

Ether hdr : 0:40:95:34:40:8d ->
0:80:ad:b:b:4b [ether_type=ip (2048)]
Ip hdr : 62.158.170.2 -> 62.44.103.64
[hl=20,version=4,tos=22,len=185,id=125
82,ttl=113]
Tcp hdr : 3678 -> 80 [flags=PUSH ACK,
seq=1232543859,ack=1830423927,win=9520
]
Data hdr : size=145 bytes

Data hexadecimal dump follow :
47 45 54 20 2f 6d 73 61 64 63 2f 2e 2e
25 35 63 GET /msadc/..%5c
2e 2e 2f 2e 2e 25 35 63 2e 2e 2f 2e 2e
25 35 63 ../..%5c../..%5c
2f 2e 2e 35 35 2e 2e 2f 2e 2e 63 31 2e
2e 2f 2e /..55../..c1../.
2e 2f 2e 2e 2e 2f 77 69 6e 6e 74 2f 73
79 73 74 ./.../winnt/syst
65 6d 33 32 2f 63 6d 64 2e 65 78 65 3f
2f 63 2b em32/cmd.exe?/c+
64 69 72 20 48 54 54 50 2f 31 2e 30 0d
0a 48 6f dir HTTP/1.0..Ho
73 74 3a 20 77 77 77 0d 0a 43 6f 6e 6e
6e 65 63 st: www..Connnec
74 69 6f 6e 3a 20 63 6c 6f 73 65 0d 0a
0d 0a 6e tion: close....n
65 63 74 69 6f 6e 3a 20 63 6c 6f 73 65
0d 0a 0d ection: close...
0a .
```

Това, което е нужно да се извади от тази порция информация, добавяна всеки път при детектиране на лоша заявка, е да се извлече реда започващ с "Ip hdr" и той да се обработи така, че от него да се извлече първия IP адрес (напр. в горния пример това е 62.158.170.2). След това информацията за този адрес трябва да се подаде на инсталирания на текущия рутер мрежови филтър, за да може да се спрат всички заявки от този адрес, както тези предназначени за адреса на рутера, така и тези предназначени за адреси, които той рутира.

Решение на проблема

За следене на лошите заявки в реално време се използва инструмента tail с опция -f, който регистрира всяка нова промяна в журналния файл prelude.log. След това потокът от tail -f се подава на обработващ скрипт. Скриптът е написан на Perl и в него става цялата обработка на данните, включително предаването на IP адреса на източника на лоши заявки към мрежовия филтър.

Идеята, заложена в написването на скрипта е следната. В постъпващата от tail -f информация се търси ред, който да съдържа низа Ip hdr. След намирането на този ред той се подлага на обработка, която включва разделянето му на полета чрез сепараторите : и ->. Очевидно е (от формата на информацията в журналния файл prelude.log), че IP адреса на източника на лошите заявки попада точно между тези два сепаратора и така се извлича като низ (стринг). След като вече е отделено това поле, то може да се предаде на IPTABLES. При включване в мрежовия филтър IPTABLES се използва включване на правилото преди другите за дадена верига с помощта на -I. Ако бъде прибавен в края на дадената верига с –A, то няма да влезе в сила, ако преди него има други правила, които позволяват лошите заявки да бъдат пропускани.

Необходимо е да се направи и проверка дали даден IP адрес, който ще се прибавя, вече не е прибавен, за да не се повтаря една и съща политика за един IP адрес в рамките на дадена верига. За целта се създава база от данни, която се съхранява във файл. Когато в prelude.log се създаде нов запис за нарушител и се извлече неговия IP адрес, то се прави проверка дали адреса вече не е попадал в базата от данни. Ако е попадал там, не се прави повикване на мрежовия филтър, за да не се повтаря записа. След тази проверка GUI приложение уведомява потребителя за прихванатия ‘лош’ адрес и го пита дали да бъде блокиран т.е. дали да се подаде на мрежовия филтър.

Процесът, който ще изпълнява този скрипт, трябва да премине във фонов режим.

Заключение

Използваната в настоящата работа система за откриване на нарушители Prelude предлага широки възможности за развитие, което й гарантира дълго присъствие на пазара. Prelude IDS развива своя подсистема за контрамерки, която позволява работа с активни отговори (active response), получени автоматично в резултат на новопоявило се съобщение за атака. Така става възможно спиране на атака, която е започнала, или предотвратяване достъпа на известни ‘враждебно-настроени’ хостове до защитената мрежа.

Цитираните по-горе възможности, както и разработеният скрипт за филтриране на лоши пакети показват, че Prelude успешно отговаря на появилите се нужди от системи за защита от нарушители IPS (Intrusion Prevention Systems). Може да се направи заключението, че Prelude е един некомерсиален IDS продукт с IPS характеристики, който успешно се използва за осигуряване сигурността на дадена мрежа и отговаря на съвременните изисквания за такива продукти [4, 5, 6, 7, 8].

Литература

1. Prelude official site: http://www.prelude-ids.org
2. Bace R., Mell P., "Intrusion Detection Systems", NIST Special Publication on IDS, http://csrc.nist.gov/publications, Nov 2001.
3. Bace R., "An Introduction to Intrusion Detection and Assessment: for System and Network Security Management", ICSA White Paper, 1998.

4. Zaraska K., "IDS Active Response Mechanisms: Countermeasure Subsytem for Prelude IDS", Technical Report (2002)
5. Zaraska K., " Prelude IDS: current state and development perspectives ", Technical Report (2003)
6. Blanc M., Oudot L., Glaume V., "Global Intrusion Detection: Prelude Hybrid IDS," Technical Report (2003)
7. Scarfone K., Mell P., “Guide to Intrusion Detection and Prevention Systems (IDPS). Recommendations of the National Institute of Standards and Technology.”
8. Tambrin C., “Integration of Intrusion Detection Systems (IDS) in Network Management”, 2002
9. http://lcpe.uni-sofia.bg/linuxdoc/prelude/

Препоръчана за публикуване
от Редакционен съвет