Windows'owy, sieciowy system wykrywania włamań SNORT

zintegrowany z systemem baz danych i narzędziem do analizy informacji

wybrane zagadnienia

1. Czym jest system wykrywania włamań IDS, jak działa?

IDS (intrusion detection system) to narzędzia przeprowadzające detekcję naruszenia bezpieczeństwa systemu w czasie rzeczywistym.

Istnieją dwa typy systemów IDS:

- **system oparty na zbiorze zasad** – w działaniu podobny do oprogramowania antywirusowego - istnieje baza sygnatur, czyli pewnych cech znanych ataków naruszających bezpieczeństwo. Pakiet przychodzący jest analizowany przez program IDS i następnie porównywany z sygnaturami. Kiedy istnieje podobieństwo pakiet traktowany jest jako źródło ataku i IDS generuje odpowiednie działanie. Podstawową wadą jest fakt, że baza danych musi być często aktualizowana;
- **systemy adaptacyjne** – wykorzystują bardziej złożone techniki aniżeli powyższe, potrafią nie tylko korzystać z wbudowanej bazy, ale także wykorzystując sztuczną inteligencję - uczą się nowych typów ataków. Wymagają jednak od administratora sporej wiedzy z zakresu matematyki i statystyki.

Bazę sygnatur można aktualizować korzystając ze specjalnych narzędzi przeznaczonych do okresowej, automatycznej aktualizacji (np. Oinkmaster dla Snort), samodzielnie – analizując działanie najnowszych exploitów - programów wykorzystujących dziury w oprogramowaniu w celu uzyskania zasobów komputera np. uprawnień administratora i odpowiednim ich opisywaniu w języku zrozumiałym dla systemu IDS. Proces ten można zautomatyzować wykorzystując skaner bezpieczeństwa systemu np. Nessus, który ma zakodowane różne typy ataków.

Istnieje także podział ze względu na podejście do włamań:

- **reakcyjny** – to rozbudowany system rejestrowania zdarzeń, alarmuje gdy atak nastąpił;
- **profilaktyczny** – reaguje już w czasie dokonywanego ataku

2. Środowisko testowania sieciowego systemu IDS

2.1 Dlaczego Virtualbox

SNORT jest sieciowym systemem wykrywania włamań i oczywiste jest, że testowanie jego działania jest możliwe tylko na maszynie podłączonej do sieci. Założeniem tego materiału jest stworzenie środowiska do testowania SNORTa na komputerze niepodłączonym do sieci, a nawet nieposiadającym jakichkolwiek interfejsów sieciowych (niewliczając loopback). Jednym z rozwiązań jest uruchomienie wirtualnej maszyny.

Z wirtualną maszyną każdy zapewne kojarzy program Microsoft Virtual PC, który umożliwia przetestowanie systemu wykrywania włamań ale w nieoptymalny sposób. Mianowicie będzie to możliwe, ale jedynie z wykorzystaniem dwóch wirtualnych maszyn – jedna, na której będzie nasłuchiwał SNORT – druga jako komputer atakującego. Dzieję się tak dlatego, gdyż adapter sieciowy w wersji „Local only" umożliwia komunikację tylko i wyłącznie między maszynami wirtualnymi. Istnieje możliwość uruchomienia jednej maszyny wirtualnej Microsoft Virtual PC, ale maszyna musi być podłączona do sieci LAN i wykorzystując fizyczny adapter komputera możemy uruchomić kolejny komputer tej sieci.

Istnieje jednak alternatywa, która rozwiązuje problem i umożliwia w pełni przetestować NIDS uruchamiając tylko jedną maszyna wirtualną na komputerze, który może nie posiadać jakiegokolwiek sprzętu sieciowego. Jest to multiplatformowy VirtualBox w wersji darmowej do użytku prywatnego. Istnieje także wersja na licencji GPL dostępna na systemy typu UNIX z kodem źródłowym. Plik instalacyjny można sciągnąć ze strony:

http://www.virtualbox.org/wiki/Downloads

2.2 Instalacja, konfiguracja i uruchomienie wirtualnej maszyny i sieci

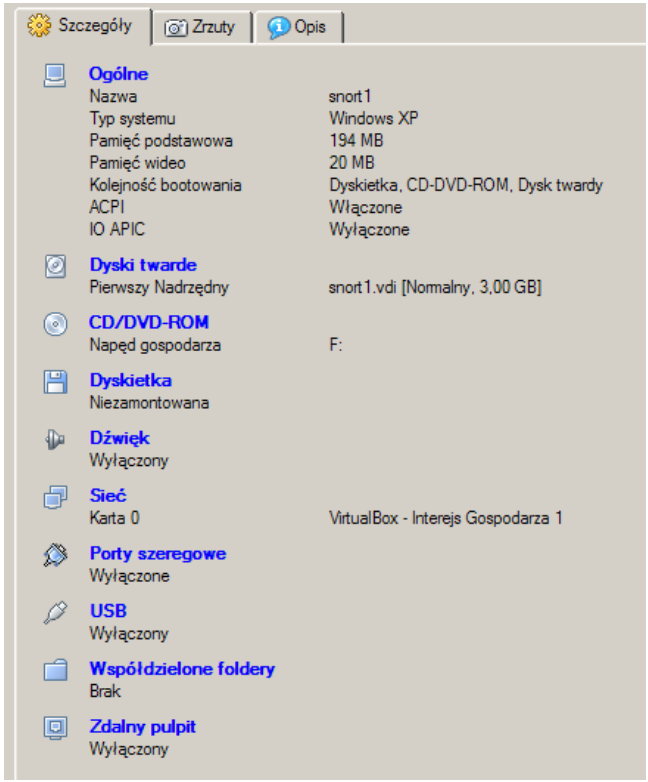
2.2.1 Instalacja maszyny wirtualnej z nowym dyskiem:

- klikamy przycisk N**owa** w górnym pasku
- wpisujemy nazwę wirtualnej maszyny i wybieramy typ systemu operacyjnego - windows XP
- przydzielamy odpowiednią ilość pamięci RAM maszyny, co najmniej 150MB – w zależności od ilości posiadanej pamięci w komputerze
- klikamy przycisk **nowy** w celu utworzenia nowego dysku wirtualnego
- zostawiamy zaznaczoną opcję „**dynamicznie rozszerzany dysk**”
- wpisujemy nazwę wirtualnego dysku i wybieramy rozmiar wirtualnego dysku
- zakańczamy proces tworzenia wirtualnego dysku – przycisk **zakończ**
- utworzony dysk będzie widoczny na liście, kontynuujemy tworzenie wirtualnej maszyny – przycisk **dalej**
- sprawdzamy poprawność danych i zakańczamy proces tworzenia wirtualnej maszyny – przycisk **zakończ**

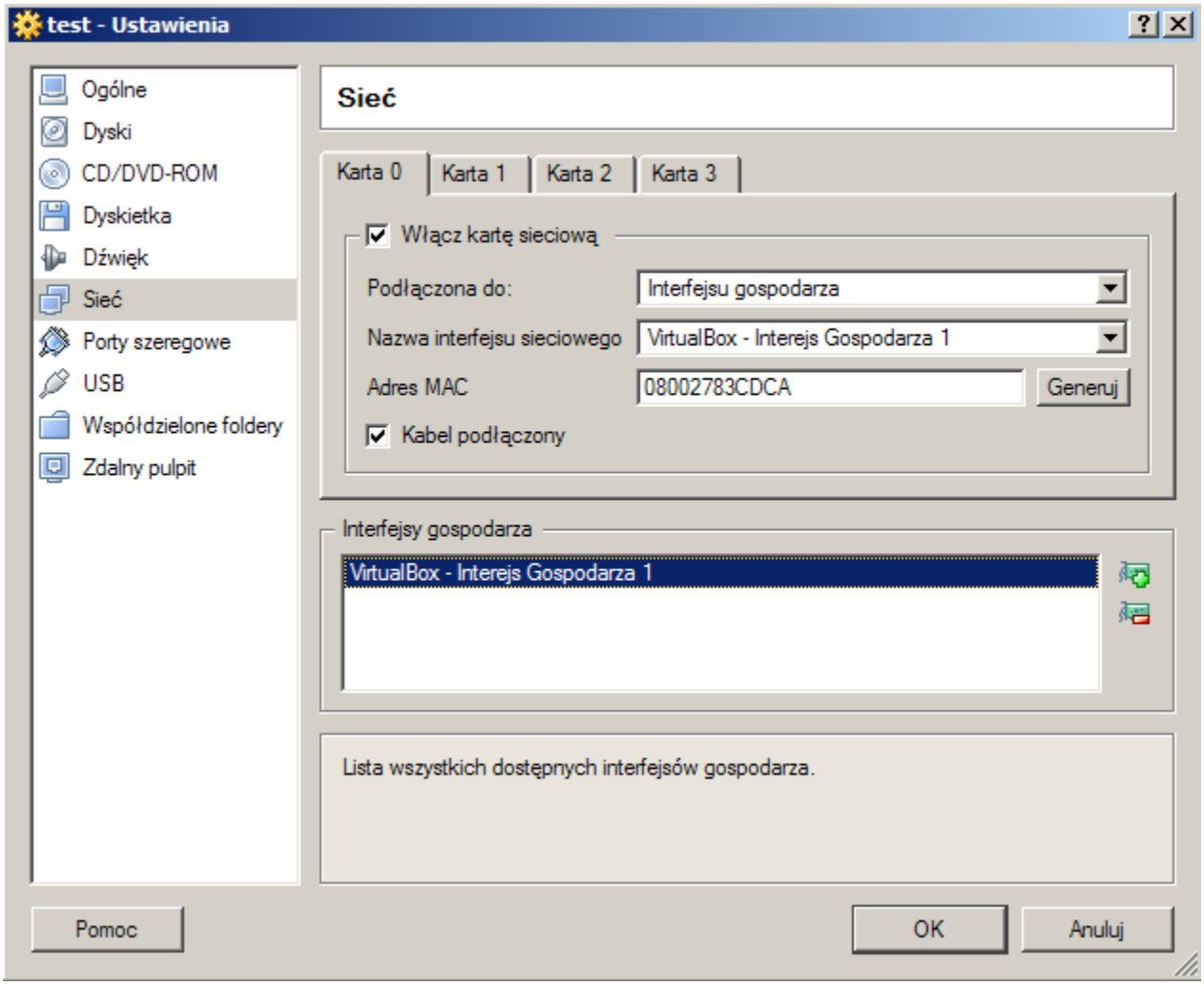
2.2.2 Ustawienia

Aby dokonać ustawień należy wybrać wirtualną maszynę a następnie kliknąć przycisk **Ustawienia.**

Powinny wyglądać podobnie do tych, które przedstawia poniższy rysunek:

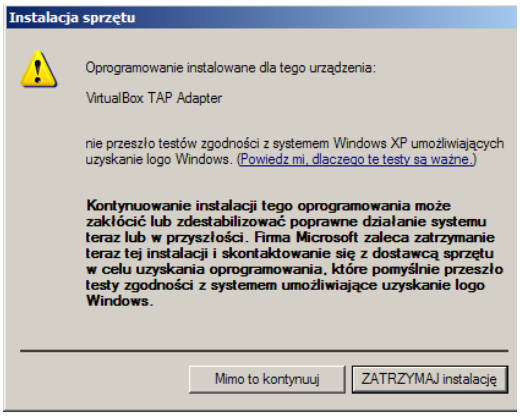


Najważniejsza jest sekcja Sieć:



Aby dodać interfejs gospodarza należy kliknąć ikonkę **+** znajdującą się w sekcji „**Interfejsy gospodarza**”, następnie wybrać nazwę dla interfejsu i kliknąć OK.

Pojawi się okno:



Wybieramy „Mimo to kontynuuj”, nastąpi proces instalacji interfejsu gospodarza.

2.2.3 Konfiguracja interfejsu gospodarza

panel sterowania -> połączenia sieciowe -> prawy myszy, właściwości -> właściwości protokołu TCP/IP

Adres IP: 192.168.1.100
Maska: 255.255.255.0

2.2.4 Uruchomienie wirtualnej maszyny i instalacji systemu

Wkładamy bootowalną płyte instalacyjną systemu Windows XP do napędu, uruchamiamy wirtualną maszynę podwójnym kliknięciem, nastąpi wystartowanie programu instalacyjnego i standardowa procedura instalacji systemu.

UWAGA: Należy uważnie przeczytać informacje o klawiszach służących do przełączania między maszynami.

2.2.5 Konfiguracja interfejsu sieciowego maszyny wirtualnej

Adres IP: 192.168.1.200
Maska: 255.255.255.0

2.3 Testowanie wirtualnej sieci

Przed przetestowaniem funkcjonowania wirtualnej sieci należy upewnić się, że żądania ECHO protokołu ICMP na wbudowanym, systemowych firewallu (o ile jest aktywny na interfejsie) są zezwolone. Następnie z drugiego komputera można przeprowadzić test połączenia: ping adresip. Otrzymana odpowiedź oznacza prawidłową instalację wirtualnej maszyny i sieci.

3. Podstawowe zasady bezpieczeństwa systemu operacyjnego

Zanim komputer stanie się właściwym elementem systemu bezpieczeństwa sieci należy przyjrzeć się systemowi operacyjnemu, na którym pracuje maszyna będąca firewallem czy stanowiąca system wykrywania włamań. Opisywany system IDS jest bazowany na Windows XP, ale reguły tutaj podane są w większości uniwersalne i można je także stosować w innych systemach operacyjnych.

Elementarną zasadą jest ograniczony dostęp osób niepowołanych do maszyny. Rozwijając ten wątek należy zwrócić uwagę aby nie isniała możliwość wyłączenia czy zrestartowania maszyny, a także aby start był możliwy tylko z jednego nośnika by wyeliminować wszelkie próby ładowania innego systemu operacyjnego, bądź dodatkowego oprogramowania.

Oprogramowanie, które stanowi pełen system IDS SNORT zajmuje około 60MB. Jest to serwer Apache, który w połączeniu z PHP służy do przetwarzania informacji zawartych w bazie danych MySQL, w której będą przechowywane logi,alerty, czyli informacje generowane przez SNORT'a. Ważne w tym momencie jest by przed instalacją systemu operacyjnego odpowiednio podzielić dysk. W przypadku winXP za absolutne minimum należy uznać dwie partycje (oczywiście system plików to NTFS): jedna przeznaczone na system operacyjny wraz z oprogramowaniem, druga na informacje generowane przez SNORT'a, czyli na bazę MySQL. Rozsądnym rozwiązaniem jest trzecia partycja przeznaczona na katalog htdocs (np skrypt BASE napisany w PHP) serwera WWW, można także wyodrębnić logi systemowe.

W większości przypadków świeżo zainstalowany system nie jest domyślnie nastawiony na bezpieczeństwo danych. Dotyczy to sporej grupy systemów operacyjnych Linux, nie wspominając już o Windows XP. Można stwierdzić, że im system bardziej user-friendly, tym mniej bezpieczny.

Należy podjąć działania mające na celu zwiększenie bezpieczeństwa świeżo zainstalowanej kopii XP:

- ustawić domyślną politykę mocnych haseł, tzn mających co najmniej 8 znaków, będących kombinacją wielkich i małych liter, cyfr oraz znaków specjalnych np. (!@#*...)

  panel sterowania -> narzędzia administracyjne -> ustawienia zabezpieczeń lokalnych -> zasady konta -> zasady haseł

- zmienić nazwę użytkownika Administrator oraz wyłączyć konto Gościa (usunięcie jest niemożliwe)

  panel sterowania -> narzędzia administracyjne -> ustawienia zabezpieczeń lokalnych -> zasady lokalne -> opcje zabezpieczeń

- usunąć wszystkie pozostałe konta

  panel sterowania -> narzędzia administracyjne -> zarządzanie komputerem -> użytkownicy i grupy lokalne -> użytkownicy

- usunąć zbędne oprogramowanie, należy przestrzegać nastepującą zasadę: **w systemie powinno być tylko to co jest naprawdę niezbędne, każdy kolejny program to potencjalna dziura**

- wyłączyć wszystkie niepotrzebne serwisy (usługi)

  informacje: http://www.blackviper.com/WinXP/servicecfg.htm

- usunąć niepotrzebne protokoły, w przypadku SNORTa wystarczy tylko TCP/IP
- włączyć usługę aktualizacji automatycznych (najlepszym rozwiązaniem jest uprzednie przetestowanie aktualizacji na innej maszynie)

- sprawdzić, czy nie są przypadkiem aktywne inne usługi sieciowe: *netstat -abo*

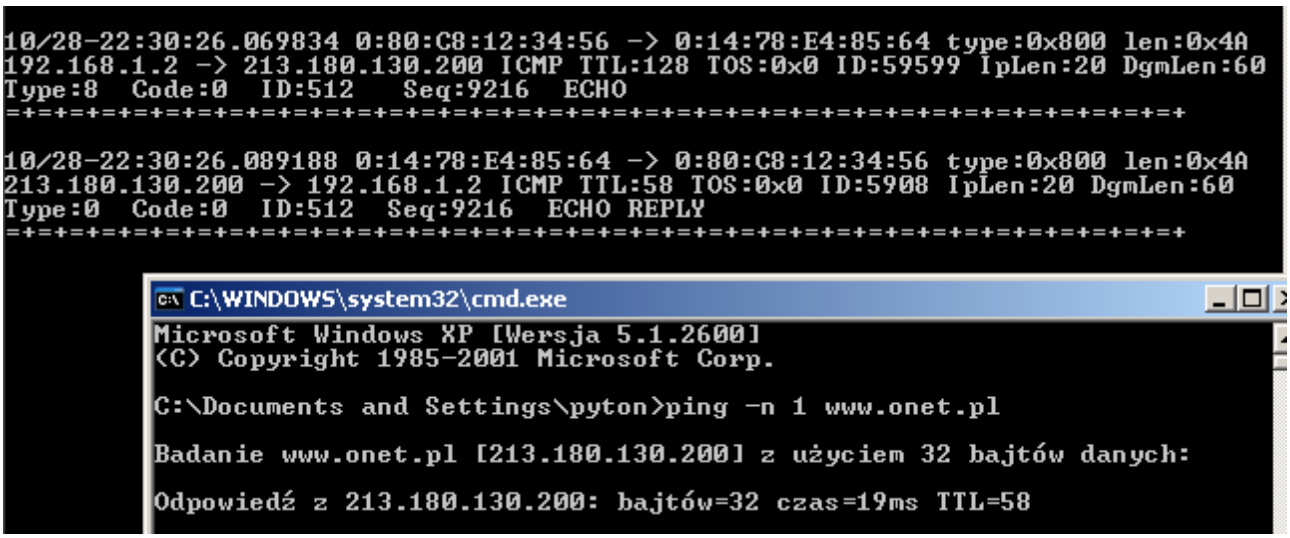
Powyższe czynności to zupełnie podstawowe kroki zwiększające bezpieczeństwo systemu Windows XP. Warto ponownie wspomnieć, ze nawet najlepsze systemu zabezpieczeń nie będą skuteczne jeśli nie zadba się o bezpieczeństwo na poziomie podstawowym. Należy pamiętać, ze nie ma systemów pozbawionych błędów – ich wykrycie jest kwestią czasu, choć są pewne wyjątki (np. QMail). Więcej informacji na temat ochrony systemu Windows znajduje się w dokumencie: *Windows XP Security Guide*, opracowanym przez Microsoft.

4. Snort – podstawowe informacje

SNORT to (NIDS – network IDS) - program typu open-source, docelowo stworzony na systemy UNIX, ale także dostępny dla systemu WINDOWS. Potrafi przeprowadzać analizę pakietów, wyszukiwać i dopasowywać podejrzane treści, a także wykrywać wiele ataków i anomalii np. ataki na serwery WWW, ukryte skanowanie portów czy próby identyfikacji systemu operacyjnego.

Działa w trzech trybach (ctrl+c przerywa pracę, argument -h: pomoc):

- **Sniffer –** przechwytuje wszystkie pakiety i wyświetla je na ekranie
  opcje (można łączyć):
  - ➔ **-v** informacje o nagłówkach pakietów TCP/UDP/ICMP
  - ➔ **-d** informacje warstwy aplikacji pakietu
  - ➔ **-e** dodatkowe nagłówki warstwy danych
  - ➔ **-w** informacje o interfejsach i ich numeracji w systemie Windows
  - ➔ **-i** <numer_interfejsu> nasłuchiwanie na konkretnym interfejsie



Rys. 1 Snort w trybie sniffer i przechwycony pakiet ICMP

- **Packet Logger –** zapisuje wszystkie przechwycone pakiety do pliku
  opcje:
  - ➔ **-l <katalog>** zapisuje do podanego katalogu tworząc hierarchię katalogów wykorzystując min adresy IP
  - ➔ **-b** zapisuje w postaci binarnej w formacie sniffera tcpdump, użyteczne w przypadku sporej ilości pakietów, możliwy późniejszy odczyt np. WireShark'iem, zapisywany jest cały pakiet, niewymagana opcja -e)
  - ➔ **-r** wyświetla na ekranie pakiety zapisane binarnie

  Zarówno w trybie *sniffer* jak i *packet logger*, aby sfiltrować dane stosuje się BPF (Berkeley Packet Filter), filtr działa na nagłówek pakietu i umożliwia zawężenie danych wyjściowych np.:

  snort -r plik.log src 192.168.1.10 and tcp dst port 80
  (odczytuj z pliku plik.log tylko te pakiety, które pochodzą od komputera o IP 192.168.1.10 i skierowane są na port 80 TCP (serwer WWW))

- **Network Intrusion Detection Mode –** najbardziej złożony tryb, właściwy dla tematu tego opracowania – sieciowy system wykrywania włamań
  opcje:
  - ➔ -c <sciezka_do_pliku> podawana jest ścieżka do pliku konfiguracyjnego

5. Instalacja systemu NIDS (SNORT)

5.1 WinPCap

WinPCap (Windows Packet Capture Library) – jest sterownikiem przechwytywania pakietów sieciowych w środowisku Windows, odpowiednikiem linuxowej biblioteki **libpcap** (http://sourceforge.net/projects/libpcap/).

Plik instalacyjny: http://www.winpcap.org/install/default.htm
(należy zainstalować wersję stabilną)

5.2 SNORT

Plik instalacyjny: http://www.snort.org/dl/binaries/win32/

Instalacje wykonujemy np. do folderu c:\Nids. W czasie instalacji pozostawiamy wszystkie domyślne ustawienia, włączając w to domyślną opcję logowania, czyli: *I do not plan to log to database, or I am planning to log to one of the databases listed above.*

Korzystając z edytora plików tekstowych (np. Notepad++ http://notepad-plus.sourceforge.net/), który prawidłowo działa na plikach systemu UNIX, wstępnie konfigurujemy SNORTA (c:\nids\etc\snort.conf). **Warto przypomnieć sobie o adresowaniu CIDR (http://pl.wikipedia.org/wiki/CIDR). Podane niżej ustawienia należy zastosować do istniejących już, wprowadzając zmianę, a także skomentowanych (należy usunąć znak #):**

var HOME_NET any
(ustalenie adresu sieci lokalnej)

var EXTERNAL_NET any
(określenie sieci zewnętrznej, z której nadchodzą ataki),

(Często ustawia się *var EXTERNAL_NET !$HOME_NET* (inna niż sieć HOME_NET), lecz na potrzeby tego ćwiczenia należy pozostawić bez zmian)

var PREPROC_RULE_PATH c:\nids\rules
var RULE_PATH c:\nids\rules
(określenie folderu z regułami ataków)

config detection: search-method lowmem
(ustawienie silnika detekcji, małe zużycie pamięci, słabe przetwarzanie)

dynamicpreprocessor directory c:\nids\lib\snort_dynamicpreprocessor
(katalog z preprocesorami dynamicznie ładowanymi)

(Preprocesory to moduły snorta odpowiedzielne za wstępną analizę pakietu pod kątem danego zagrożenia, działają „pomiędzy" modułem analizy protokołu i silniku detekcji)

dynamicengine c:\nids\lib\snort_dynamicengine\sf_engine.dll

output database: log, mysql, user=snort password=haslo2 dbname=snort host=localhost sensor_name=IDSSnort
(logowanie do bazy danych, podane hasło należy będzie powtórnie wprowadzić – więcej informacji w dalszej części)

include c:\nids\etc\classification.config
(zawiera klasyfikatory rodzajów ataków z nadanym priorytetem zagrożenia, ustawienie globalne, może być ustawiane

także lokalnie - w każdej regule)

include c:\nids\etc\reference.config
(definicja URL'i stanowiących odniesienie do słów-kluczów zawartych w regule, opcja reference)

include c:\nids\etc\threshold.conf

output alert_fast: alert.ids

Należy znaleźć wiersz:

sense_level { low }

i zamienić na:

*sense_level { low } *
logfile { portscan.log }

Należy ściagnąć najnowsze reguły ataków ze strony: http://www.snort.org/vrt/ (wymagana krótka rejestracja) - kategoria dla zarejestrowanych użytkownik dla bieżącej wersji Snorta. Następnie zawartość katalogu *rules* skopiować do katalogu *c:\nids\rules*.

Test instalacji:

W tej części sprawdzimy poprawność instalacji poprzez przechwycenie pakietów protokołu ICMP.

Uruchamiamy konsolę (windows prompt): *start -> uruchom -> cmd.exe*

Wchodzimy do katalogu plików wykonywalnych SNORTA: *cd c:\NIDS\bin*

Sprawdzamy dostępne interfejsy sieciowe (a dokładnie ich numery): *snort -W*

Uruchamiamy SNORTA w trybie SNIFFER na odpowiednim interfejsie: *snort -v -i <numer_interfejsu>* np. *snort -v -i 2*

Z drugiego komputera wysyłamy żądanie echo: ping adresIP komputera, na którym nasłuchuje SNORT. Jeżeli Snort jest skonfigurowany prawidłowo to wyświetli informacje o przechwyconych pakietach ICMP.

5.3 Instalacji serwera WWW: Apache

Plik instalacyjny: http://ftp.tpnet.pl/vol/d1/apache/httpd/binaries/win32/
(wersja stabilna 2.2, no ssl, plik MSI)

pole **network domain** może być puste, **server name** np. localhost, **administrator's email**: dowolny, instalacja jako serwis, typowa - do katalogu np. **c:\NIDS\www**

Po instalacji w systray'u powinna pojawić się ikonka: **Apache Service Monitor,** do kontrolowania serwisem serwera Apache. Z poziomu tego programu można włączać, wyłączać, restartować program. Można również kontrolować działanie usługi poprzez komendę NET, domyślna nazwa serwisu to apache2.2 (np. net start apache2.2), a także z poziomu programu wbudowanego w system **services.msc**.

5.4 Instalacja PHP

Plik instalacyjny: php5.2.4

Proponowany docelowy katalog instalacji: *c:\nids\php*
Moduł: *Apache 2.2.x Module*
Apache configuration directory: *c:\nids\www\conf*
Items to install:
Extras: *Pear Install* (system rozszerzeń dla PHP)
Extensions: *MySQL* (obsługa bazy danych MySQL),
GD2 (graficzna biblioteka)

Otwieramy plik konfiguracyjny Apache: *c:\nids\www\conf\httpd.conf*
Instalator PHP dodał na końcu pliku:
PHPIniDir "c:/NIDS/php/"
LoadModule php5_module "c:/NIDS/php/php5apache2_2.dll"

Dopisujemy jeszcze:
AddType application/x-httpd-php .php

Dopisujemy index.php by był także traktowany jako indeks katalogu:

```
<IfModule dir_module>
   DirectoryIndex index.html index.php
</IfModule>
```

Edytujemy plik konfiguracyjny PHP (c:\NIDS\php\php.ini):
include_path = "c:\nids\php\pear"
session.save_path = "c:\windows\temp"
extension=php_gd2.dll
extension=php_mysql.dll

Zalecane jest zrestartowanie komputera.

Restartujemy serwer APACHE:
net stop apache2.2
net start apache2.2

Jeżeli okaże się, że Apache nie może odnaleźć modułu php_mysql to należy skopiować plik libmysql.dll znajdujący się w folderze PHP do katalogu c:\windows\system32.

UWAGA: Należy mieć otwarty port serwera WWW: 80 TCP

Testujemy środowisko APACHE + PHP:
Zapisujemy plik o zawartości:

```
<?php
  phpinfo();
?>
```

do pliku *c:\nids\www\htdocs\test.php*

następnie wywołujemy skrypt http://localhost/test.php

Wynikiem powinno być kilka tabel z informacjami na temat stanu środowiska PHP. Należy

upewnić się, że zmiany wprowadzone w pliku konfiguracyjnym PHP są widoczne na wygenerowanej przez funkcję phpinfo() stronie. Między innymi powinna znajdować się sekcja mysql, jeżeli takowej nie ma – świadczy to o niezaładowanym module MySQL, powodem może być niewykonana czynność opisana wyżej kolorem czerwonym.

5.5 Instalacja MySQL

Plik instalacyjny: mysql-essential-5.0.45-win32.msi

Jeśli chcemy zainstalować bazę w standardowej lokalizacji wybieramy instalację *Typical*, jeśli nie *Custom* i zmieniamy scieżkę instalacji. Zostawiamy domyślnie *Configure Mysql Server now* następnie wybieramy *Standard Configuration;* zostawiamy *Install As Windows Service;* odznaczamy *Launch the Mysql Server automatically* i zaznaczamy *Include Bin Directory in Windows Path*, ustawiamy *new root password*.

Konfigurujemy bazę MySQL dla BASE (Basic Analysis and Security Engine):

mysql -u root -p	połączenie z serwerem baz jako użytkownik root
create database snort;	tworzenie bazy danych snort
create database archive;	tworzenie bazy danych archive
show databases;	sprawdzenie istniejących baz danych
connect snort;	połączenie się z bazą danych snort
source c:\nids\schemas\create_mysql	wypełnienie bazy snort zgodnie z plikiem zawartym w pakiecie Snort'a
connect archive;	połączenie z bazą danych archive
source c:\nids\schemas\create_mysql	wypełnienia bazy archive ...
grant INSERT,SELECT,UPDATE on snort. to snort@localhost identified by 'haslo2';*	utworzenie użytkownika i nadanie uprawnień na bazę snort i wszystkie jej tabele
grant INSERT,SELECT,UPDATE,DELETE,CREATE on archive. to base@localhost identified by 'haslo';*	utworzenie użytkownika base i nadanie uprawnień
grant INSERT,SELECT,UPDATE,DELETE,CREATE on snort. to base@localhost identified by 'haslo';*	

5.6 Instalacja ADOdb

ADOdb to interfejs dla PHP do komunikacji z dowolną bazą danych w ten sam sposób.

Plik instalacyjny: adodb-502-for-php [plik *.zip]

Zawartość pliku należy rozpakować do folderu c:\nids\adodb5

5.7 Instalacja BASE

Plik instalacyjny: base-1.3.8

Zawartość pliku rozpakowujemy do folderu c:\nids\www\htdocs. Tak więc, po rozpakowaniu BASE będzie znajdował się w folderze c:\nids\www\htdocs\base-1.3.8.

Otwieramy plik *c:\nids\www\htdocs\base-1.3.8\base_conf.php.dist,* następnie zapisujemy jako *base_conf.php* i edytujemy*:*

$BASE_Language = 'polish';	ustawiamy język polski
$BASE_urlpath = 'http://localhost/base-1.3.8/';	URL do BASE
$DBlib_path = 'c:\nids\adodb5';	ścieżka dostępu do ADOdb
$portscan_file = 'c:\nids\log\portscan.log';	log skanowania systemu

$alert_dbname = 'snort';
$alert_host = 'localhost';
$alert_port = '';
$alert_user = 'base';
*$alert_password = 'haslo'; /*tutaj hasło ustawione dla użytkownika snort@localhost*/*

$archive_dbname = 'archive';
$archive_host = 'localhost';
$archive_port = '';
$archive_user = 'base';
*$archive_password = 'haslo'; /*tutaj hasło ustawione dla użytkownika snort@localhost*/*

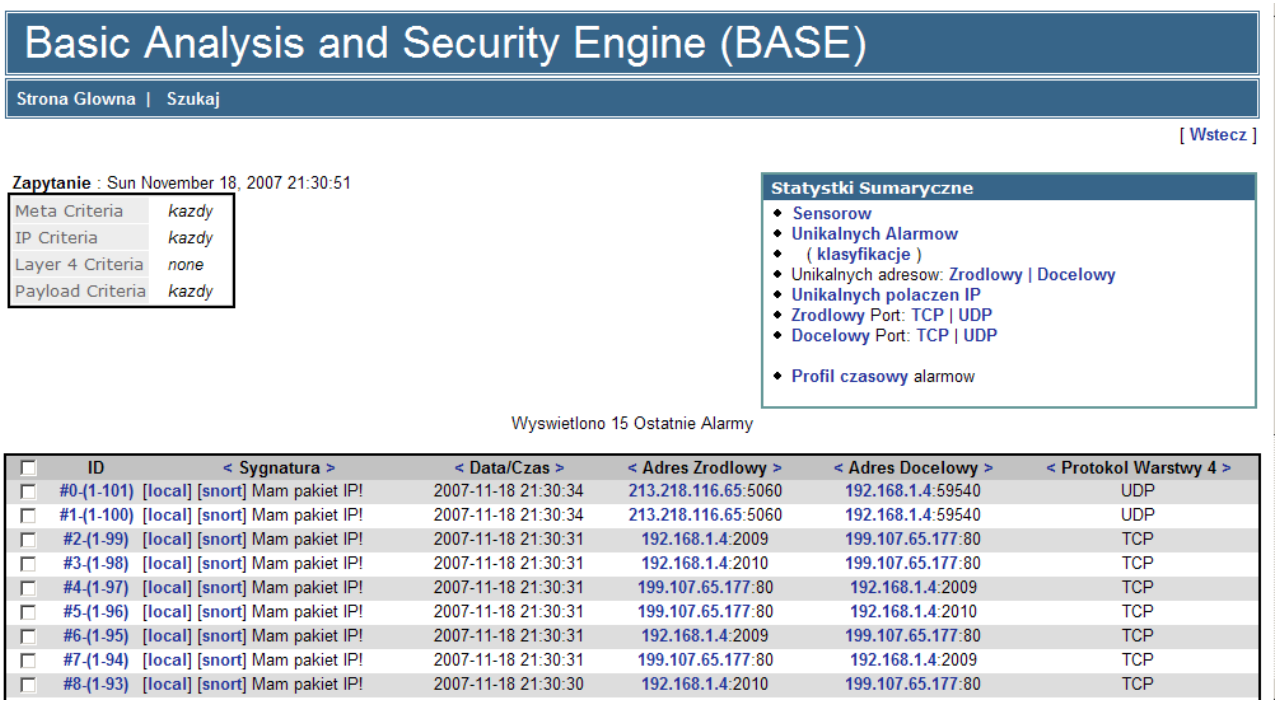
Drugi etap konfiguracji baz danych:

mysql -u root -p	
connect snort;	
source c:\nids\www\htdocs\base-1.3.8\sql\create_base_tbls_mysql.sql	
connect archive;	
source c:\nids\www\htdocs\base-1.3.8\sql\create_base_tbls_mysql.sql	

Ostatni etap, instalacja PHP PEAR i dodatkowych frameworków dla PHP:

cd c:\nids\php	
go-pear	instalacja system-wide pear, naciskamy enter jako odpowiedź na zapytanie, następnie ponownie kilkukrotnie enter
pear channel-update pear.php.net	uaktualnienie istniejącego kanału PEAR
pear install Image_Color	zarządzanie kolorami
pear install Log	narzędzia logowania
pear install Numbers_Roman	konwersja z i do numeracji rzymskiej
pear install http://pear.php.net/get/Image_Canvas	rysowanie obrazków
pear install http://pear.php.net/get/Numbers_Words-0.15.0	zamiana liczb na ich słowne odpowiedniki
pear install http://download.pear.php.net/package/Image_Graph-0.7.2.tgz	wyświetlanie danych numerycznych jako wykresy

W tym momencie jest zainstalowany pełen system, wstępnie skonfigurowane środowisko, na razie jeszcze bez danych, także nie można w pełni obserwować działania BASIS, który jest dostępny pod adresem: http://localhost/base-1.3.8/.



Rys. 2 BASE – 15 ostatnich ataków. Została dodana nowa reguła, która każdy pakiet IP traktuje jako niebiezpieczny. W ten sposób można szybko sprawdzić poprawność instalacji.

6. Reguły identyfikowania ataków

Mechanizm detekcji zagrożeń polega na porównaniu przechwyconego i zrekonstruowanego pakietu ze zbiorem reguł i podjęciu odpowiedniej akcji. Snort wykorzystuje prosty i bardzo funkcjonalny język umożliwiający określenie reguły ataku. Na dzień dzisiejszy program potrafi analizować protokoły TCP,UDP,ICMP,IP.

Reguła składa się z dwóch logicznych części: z **nagłówka** i **opcji**. Nagłówek określa akcję, protokół, źródłowy i docelowy adres IP pakietu oraz źródłowy i docelowy numer portu. Opcje (zapisane w nawiasie) umożliwiają opisanie pakietu – wskazują na cechy, które powinny być analizowane w pakiecie. Reguła nie musi być zapisana w jednym wierszu, w takim przypadku wszystkie wiersze oprócz ostatniego muszą być zakończone znakiem „\”. W dyrektywie reguły można stosować negację poprzez użycie znaku „!”.

Reguły identyfikowania ataku pozwalają na podjęcie pięciu rodzajów akcji: przepuszczenia pakietu - **pass**, zapisania informacji do dziennika - **log**, ogłoszenia alarmu - **alert**, alarmowania i podjęcia do działania innej dynamicznej reguły – **activate** i pozostanie w spoczynku do czasu aktywowania przez regułę activate, po czym działanie jako reguła log - **dynamic**, odrzuceniu pakietu przez iptables i zapisaniu informacji w logach – **drop,** bądź odrzuceniu pakietu i wysłaniu informacji TCP reset w przypadku protokołu TCP lub ICMP port unreachable jeśli jest to pakiet UDP - **reject**. Istnieje możlwość tworzenia własnych akcji.

Do określenia kierunku przepływu pakietu stosuje się znaki „->” (z lewej strony do prawej), „<-” (z prawej do lewej), „<>” (obustronnie).

Snort oprócz podania konkretnego numeru portu umożliwia określenie zakresu portów **5:6000** (od 1 do 6000), **:2000** (mniejsze lub równe 2000), **600:** (większe lub równe 600).

Opcje odseparowane są znakiem średnika, natomiast argument opcji podaje się po znaku dwukropka.

Istnieją opcję opisującę regułę: **sid** (id reguły snorta, <100 zarezerwowane, 100:100000 zarezerwowane dla dystrybucji snorta, 1000000< wykorzystywane dla lokalnych reguł), **gid** (numer generatora [modułu] snorta), **classtype** (klasa ataku – podział dostępny w dokumentacji), **metadata** (dodatkowe informacje związane z regułą), **reference** (zewnętrzne informacje na temat luki, którą opisuje reguła, np. reference:bugtraq,15250 – oznacza, że informacja o luce znajduje się w powszechnie znanym serwisie o bezpieczeństwie: www.securityfocus.com/ o bid: 15250, więcej w dokumentacji).

Reguły najlepiej zapisać w osobnym pliku np. my.rules a następnie dopisać w snort.conf:
include $RULE_PATH/my.rules

Poniższa reguła powoduje, że będa logowane wszystkie próby połączenia do komputera w sieci 192.168.1.0/24 z usługą FTP. W systemie log będzie opisany jako: „proba polaczenia z ftp”.

log tcp any any -> 192.168.1.0/24 21 (msg: „proba polaczenia z ftp”)

W regułach można wykorzystywać zmienne zapisane w snort.conf np.:

log tcp any any -> $HOME_NET 21 (msg: „proba polaczenia z ftp”)

6.1 Opcja Content

Jedną z ważniejszych opcji jest **content** - określa treść pakietu i może być powtarzana wielokrotnie. Rozróżnia wielkość liter. Dane binarne (bytecode) zapisuje się hexadecymalnie między znakami określającymi potok: „|”. Można mieszać tekst i dane binarne w jednej opcji content.

Alert w przypadku pojawienia się pakietu pochodzącego z sieci innej niż 192.168.1.0/24 oraz 10.1.1.0/24 o dowolnym porcie źródłowym i przeznaczonego dla sieci 192.168.1.0/24 bądź 10.1.1.0/24 o porcie docelowym 111 i zawartości binarnej *00 01 86 a5:*

```
alert tcp ![192.168.1.0/24,10.1.1.0/24] any -> \
[192.168.1.0/24,10.1.1.0/24] 111 (content: "|00 01 86 a5|"; \
msg: "external mountd access";)
```

6.1.1 Zmiana zachowania opcji content:

nocase;
nie rozróżnianie wielkości liter, działa dla poprzedzającej opcji content;

depth: <liczba_bajtów>
określa jak głęboko powinien być szukany wzorzec w pakiecie, np. 5 oznacza, że będzie szukany w 5 pierwszych bajtach;

offset: <liczba_bajtów>
przesuniecię względem początku pakietu, od którego będzie wyszukiwany wzorzec;

Przykład:

Pomiń 4 pierwsze bajty i szukaj w kolejnych 20 bajtach tekstu „cgi-bin/phf” :
alert tcp any any -> any 80 (content: "cgi-bin/phf"; offset:4; depth:20;)

distance: <liczba_bajtów>
ile bajtów będzie ignorowane przed przeszukaniem wzorca poprzedzającego opcję distance względem końca wzorca poprzedzającego wzorzec, dla którego działa opcja distance

Przykład:
(alertuje w przypadku odnalezienia wyrażenia regularnego /ABCDE.{1}EFGH/)
alert tcp any any -> any any (content:"ABCDE"; content: "EFGH"; distance:1;)

within: <liczba_bajtów>
zapewnia, że między wzorcami jest co najwyżej liczba_bajtów

http_client_body;
wzorzec będzie wyszukiwany w znormalizowanym ciele żądania http, działa dla poprzedzającej opcji content;

6.2 Pozostałe opcje działające na zawartości pakietu

uricontent: [!] <tekst>

WIKIPEDIA:
***URI** (ang. Uniform Resource Identifier) jest standardem internetowym umożliwiającym łatwą identyfikację zasobów w sieci. Zdefiniowany jest w dokumencie RFC 2396.*

URI jest, zazwyczaj krótkim łańcuchem znaków, zapisanym zgodnie ze składnią określoną w standardzie. Łańcuch ten określa nazwę lub adres zasobu, który dany URI identyfikuje.

URI składa się z URL (ang. *Uniform Resource Locator*) i URN (ang. *Uniform Resource Name*).

Szczególnym przypadkiem URI jest URL, który oprócz identyfikacji zasobu wskazuje również sposób dostępu do niego.

Właściwie URI jest pojęciem nadrzędnym i obejmuje URL i URN jako dwa różne sposoby reprezentacji tego samego adresu. Podstawową różnicą między nimi jest fakt, że URL z definicji wskazuje lokalizację, tj. miejsce, z którego dany zasób można ściągnąć (adres) i sposób, w jaki można to zrobić (protokół, np. http, ftp, ...). URI służy tylko do identyfikacji i niekoniecznie musi wskazywać miejsce skąd coś można ściągnąć. Standardowo URI strony www (np. http://www.wikipedia.org) jest utożsamiany z jej URL. Stąd wynika fakt, że te dwa terminy są często używane zamiennie.

Opcja umożliwia wyszukiwanie wzorca w znormalizowanym URI.
Dla przykładu poniższe URI:

/scripts/..%c0%af../winnt/system32/cmd.exe?/c+ver

w wersji znormalizowanej:

/winnt/system32/cmd.exe?/c+ver

albo

/cgi-bin/aaaaaaaaaaaaaaaaaaaaaaaa/..%252fp%68f?

będzie

/cgi-bin/phf?

Dla nieznormalizowanej wersji należy użyć opcji content;

urilen [<,>] <liczba_bajtow>
określa długość URI

np. urilen < 5; urilen 5<>10, urilen > 10

isdataat:<bajt>[,relative];

Jeśli istnieje potrzeba przeszukania zawartości pakietu przy użyciu wyrażeń regularnych, należy zainteresować się opcją **pcre**, natomiast szeroki wachlarz operacji na bajtach oferuje opcja **byte_test,** dokładniejszym testowaniem przepływu danych po reassemblacji strumienia pakietów TCP zajmuje się opcja **flow**.

7. Ćwiczenie

Celem ćwiczenia (oprócz zbudowania systemu NIDS) jest wykonanie ataków SQL Injection na dołączony do opracowania skrypt PHP - przeanalizowanie techniki i napisanie reguł dla systemu NIDS Snort, który w przypadku ich ponownego wykorzystania będzie generował alert.

Do ćwiczenia dołączone są:

- **baza.sql** – źródło bazy danych, na której będzie wykonywany atak;
- **sqlinjection.php** – skrypt PHP podatny na opisywany atak, docelowo służący do zmiany hasła podanego użytkownika;
- **exploit.jar, exploit.exe –** przykładowy program JAVA'y wykorzystujący błąd w sqlinjection.php;
- **testpassword.php –** skrypt do sprawdzenia działania exploit'a, a konkretniej poprawności hasła użytkownika;

7.1 SQL Injection

To technika nieautoryzowanego uzyskiwania i modyfikowana danych działająca na wartwę danych, którą stanowi np. baza danych SQL. Atak wykorzystuje błędy programisty (nie odpowiednie filtrowanie danych wejściowych np. wpisanych w formularzach) w dynamicznie generowanych aplikacjach internetowych (PHP, ASP, JSP), które działają na danych zawartych w bazach danych np. MySQL, MSSQL, Oracle. Atakujący wykorzystując tą technikę – wstrzykując złośliwy kod może uzyskać wiele informacji o systemie operacyjnym a w szczególnych przypadkach przejąć całkowitą kontrolę nad nim. Atak mocno związany jest z implementacją składni serwera baz danych, im większą elastycznościa charakteryzuje się serwer tym bardziej ułatwia jego wykonanie.

Więcej informacji można znaleźć na stronach:
http://pl.wikipedia.org/wiki/SQL_injection
http://republika.onet.pl/20405,16594,7,04,kursy.html
http://www.imperva.com/application_defense_center/white_papers/blind_sql_server_injection.html
http://www.unixwiz.net/techtips/sql-injection.html
http://www.poradnik-webmastera.com/artykuly/bazy_danych/sql_injection.php
http://anakin.us/blog/przepis_na_sql_injection/

7.2 Przygotowanie środowiska

Należy utworzyć bazę danych **testdb**, następnie utworzyć użytkownika **testdbuser@localhost**, który będzie miał uprawnienia CREATE,DELETE,DROP,SELECT,INSERT,UPDATE na bazę **testdb** i hasło **testdbuser**. Wypełnić bazę wykorzystując skrypt baza.sql

7.3 SQL Injection w praktyce

7.3.1 sqlinjection.php służy do zmiany hasła użytkownika w testowej bazie danych. Autoryzacja odbywa się poprzez stare hasło. Standardowe hasła są znane – **baza.sql**. Należy upewnić się czy faktycznie są poprawne – użycie skryptu **testpasswords.php** rozwieje tę wątpliwość.

Zmiana hasłą użytkownika bez znajomości starego jest niemożliwa. Czy na pewno? Należy przeanalizować kod PHP, w szczególności zapytanie odpowiedzialne za aktualizację hasła.

Dostrzegasz jakieś błędy w kodzie? Są i to poważne. Aby się przekonać, że wcale nie trzeba znać starego hasła przeanalizuj kod exploit'a. Następnie użyj go by zmienić hasło użytkownika zapisanego w testowej bazie. Jeśli po wykonaniu programu Twoim oczom ukazał się tekst „ok!", oznacza to nic innego jak bardzo prosty atak SQL i w konsekwencji zmiana hasła.

Nadszedł odpowiedni moment by jeszcze bardziej zagłębić się w tematykę SQL Injection.

UWAGA: W PHP istnieją mechanizmy zabezpieczające przed atakami SQL Injection. Na większości profesjonalnych serwerów metody tutaj opisywane mogą nie być skuteczne. Opracowanie ma na celu min zapoznanie z ideą ataków SQL Injection.

7.3.2 Napisz swój program, lub opisz jak uzyskałbyś **ID** użytkownika magda.

7.4 Reguły do SQL Injection

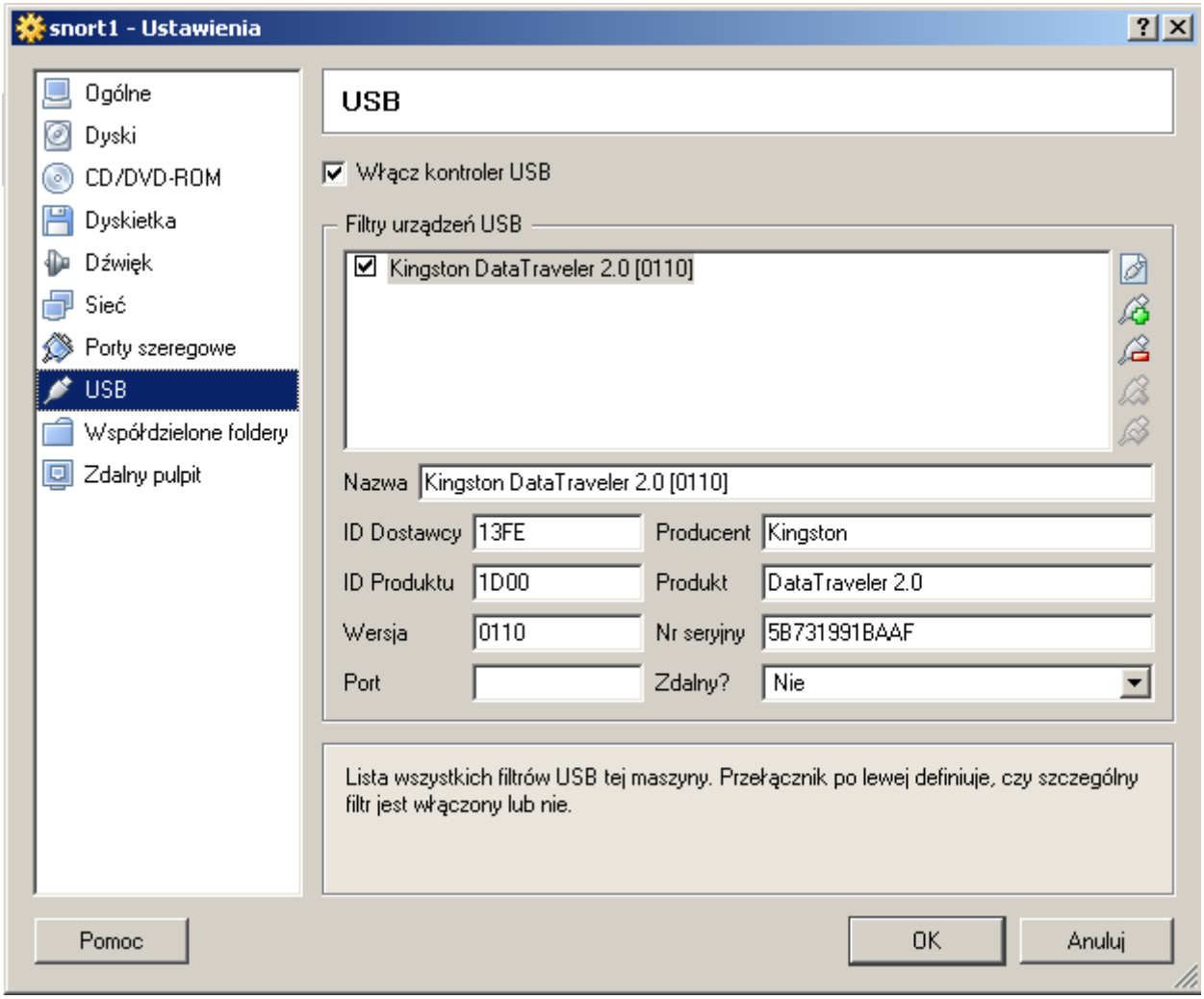
7.4.1 Napisz regułę, która będzie generować alerty: „sqlinjection.php -> exploit.jar", w przypadku wykonania exploita. Reguła ma dotyczyć działania tylko i wyłącznie programu exploit dla dowolnych argumentów. Ma więc dotyczyć konkretnego klienta protokołu (zobacz jak zbudowane jest zapytanie http) i przeanalizuj (najlepiej wykorzystując wireshark) pakiety przechwycone w trybie packet logger. Reguła ma nie działać dla manualnego ataku z poziomu przeglądarki internetowej. Zakwalifikuj atak do klasy web-application-attack. Reguła jest nieoficjalna, nadaj odpowiedni identyfikator. Atak nadchodzi z sieci zewnętrznej do wewnętrznej – domowej.

8. Sprawozdanie

Powinno zawierać:
- Screen'y obrazujące zrealizowaną sekcję (każdy element) opisywanego systemu IDS.
- Screen z wykonania programu exploit.
- Rozwiązanie zadania 7.3.2, 7.4.1 (włącznie ze screen'em z BASE).

9. Inne

Istnieje możliwość użycia pendrive'a w celu skopiowania na maszynę wirtualną potrzebnych plików. Należy uruchomić kontroler USB:



9. Dalsza lektura

http://www.snort.org
oficjalny serwis

http://searchsecurity.techtarget.com/general/0,295582,sid14_gci1083823,00.html
praktyczne informacje na temat SNORT'a

http://www.winids.com
serwis traktujący o budowaniu IDS'ów dla Windows

http://pl.docs.pld-linux.org/uslugi_snort.html
dużo informacji o SNORT'cie w języku polskim