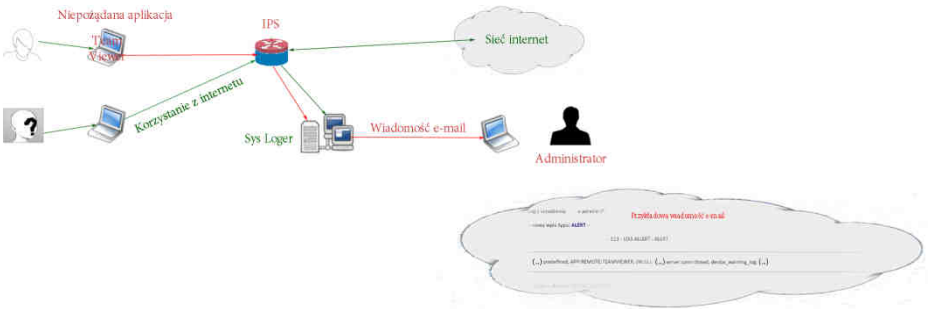
SysLoger

Instrukcja obsługi



maj 2018
dla wersji aplikacji 2.1.0.1
(wersja dokumentu 2.5)

Spis treści:

Wykaz załączników:

Wprowadzenie

Program Sys Loger jest aplikacją działającą w systemie Windows. Podstawowym zadaniem programu jest:

- **archiwizacja otrzymanych logów z urządzeń**,
- analiza treści ujętych w logach według założonych filtrów (pułapek) oraz informowanie o ich wystąpieniu w sposób ciągły,
- wykrywanie ataków DDoS na podstawie ilości wpisów w czasie oraz wielkości logu pliku tekstowego,
- codzienne i miesięczne raportowanie według założonych filtrów,

program dodatkowo umożliwia:

- na bieżące analizowanie dostępności wskazanych urządzeń w sieci,
- zdalne sprawdzanie dostępności urządzeń,
- wykonanie automatycznych kopii konfiguracji z urządzeń sieciowych wraz z obsługa zdalnego repozytorium,
- skanowanie zasobów sieciowych (ręczne, automatyczne) wraz z raportowaniem pełnym oraz przyrostowym.

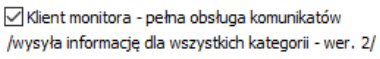
Konfiguracja urządzeń nie jest elementem niniejszej instrukcji.

Dzięki **bieżącej analizie** oraz ostrzeganiu **spełniony jest jeden z wymogów Rekomendacji D KNF** mówiący o konieczności ciągłego przeglądania zapisów jakie są rejestrowane na urządzeniach sieciowych.

(…)

Od wersji 2.0.0.4 uruchomiono współpracę **z wersją www klienta monitora**.

Od wersji 2.0.0.4 uruchomiona została druga pełna obsługa komunikatów dla klienta monitora. Konieczne jest zaznaczenie w zakładce Opcje -> Ogólne -> Ogólne opcji „Klienta monitora – pełna obsługa komunikatów.



Funkcjonalność

Moduły wchodzące w skład programu i ich funkcjonalności:

1. **Monitor programu** – okno programu prezentujące otrzymywane logi z urządzeń. W celu działania niezbędne jest dokonanie konfiguracji oraz uruchomienie serwisów:
   a) Syslog Serwis,
   b) Nasłuch serwis

   Monitor dokonuje bieżącej analizy otrzymanej informacji. Możliwe jest zdefiniowanie praktycznie dowolnej pułapki na podstawie analizy otrzymanej treści. Udostępnione zostały w programie opcje wyjątków, opcje analizy ataków typu **DDoS** w tym **flood**owania (kontrolowana jest ilość w czasie) oraz inne opisane w części poświęconej konfiguracji.

Zrzut ekranu monitora programu odpowiedzialnego za bieżącą analizę logów, umożliwia konfigurację programu.

2. **Syslog serwis** – serwis systemu Windows odpowiedzialny za odbiór i archiwizację logów z urządzeń. Odbiór logów następuje domyślnie na porcie 514. Serwis przekazuje informacje na zdefiniowanym porcie do monitora programu. Logi mogą być zapisywane do plików tekstowych i/lub do bazy MySQL. Zalecanym formatem zapisu są plik tekstowe.

3. **Raport serwis** – serwis systemu Windows odpowiedzialny za generowanie codziennych zbiorczych raportów i ich przesyłanie pocztą e-mail.

4. **Ping serwis** – serwis systemu Windows odpowiedzialny za sprawdzanie łączności wybranych urządzeń w sieci.

5. **Nasłuch serwis** – serwis systemu Windows odpowiedzialny za restart monitora oraz usług SysLoger'a. Wymagane jest uruchomienie serwisu z zaznaczoną opcją resetu programu SysLoger – usługa kontroluje wyłączenie monitora oraz pozostałych usług w minutowych odstępach czasu, w przypadku wyłączenia uruchamia monitor i usługi automatycznie. Dodatkowo o wskazanej godzinie dokonywany jest jeden pełen restart wszystkich zainstalowanych usług oraz monitora. Serwis nasłuchu odpowiedzialny jest ponadto za odbiór i wykonanie zdalnych poleceń wysyłanych z uprawnionych adresów e-mail (na przykład kontrola łączności za danym urządzeniem.

(…)

Funkcjonalności modułu Monitora:

- zapis logów do pliku tekstowego i/lub bazy MySQL,
- definiowanie numeru portu nasłuchu programu (globalnie dla wszystkich urządzeń),
- definiowanie ilości wpisów w oknie logu,
- bieżące monitorowanie i powiadamianie o przekroczeniu parametru granicznej wartości wolnego miejsca,
- wykrywanie ataków DDoS (floodowania)

  - monitoring wartości granicznej wielkości logu tekstowego,

  - monitoring ilości wpisów z urządzeń (dla każdego urządzenia prowadzony jest oddzielny monitoring ilości wpisów w czasie),
- definiowanie urządzeń od których otrzymywane są logi i dla których prowadzony jest monitoring,
- definiowanie opcji powiadamiania

  - dla kategorii (alert, critical, terror, warning, notise, info, debug),

  - dowolnego tekstu wykrytego w otrzymywanych logach

  (…)

Wymagania

Wymagania sprzętowe:

- system operacyjny minimum MS Windows XP,
- komputer Core 2 Duo lub szybszy,
- pamięć ram minimum 1 GB,
- wolne miejsce na dysku twardym – w zależności od ilości urządzeń oraz ich konfiguracji w zakresie przekazywanych informacji w logach. Sugerowane minimum 40GB.

Sprawne wyszukiwanie logów, generowanie raportów wymaga zastosowania możliwie szybkiego sprzętu, w przypadku wirtualizacji zadeklarowania odpowiednich parametrów.

Instalacja, inicjacja wersji

Instalacja podstawowa:

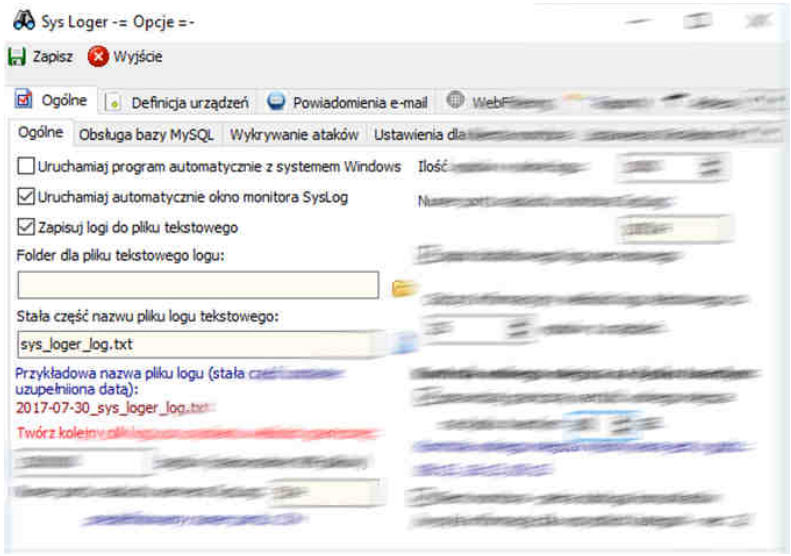
Instalację programu przeprowadzamy wypakowując otrzymane archiwum w dowolnym miejscu na twardym dysku. Zalecane jest utworzenie bezpośrednio na danym dysku katalogu (na przykład sysloger) i wypakowania do niego zawartości archiwum.

Po wypakowaniu do katalogu głównego z plikami należy wkopiować plik licencji.

(…)

Konfiguracja i uruchomienie

Konfigurację programu SysLoger przeprowadza się po wybraniu menu Opcje z monitora sys_loger.exe



Wskazanie nieistniejącego folderu dla zapisu pliku tekstowego logu spowoduje zmianę katalogu na podkatalog „logi” znajdujący się w katalogu z programem. W efekcie program będzie działał pomimo wskazania nieprawidłowego katalogu zapisu logu. Kontrola katalogu następuje podczas uruchomienia serwisu syslog’a.

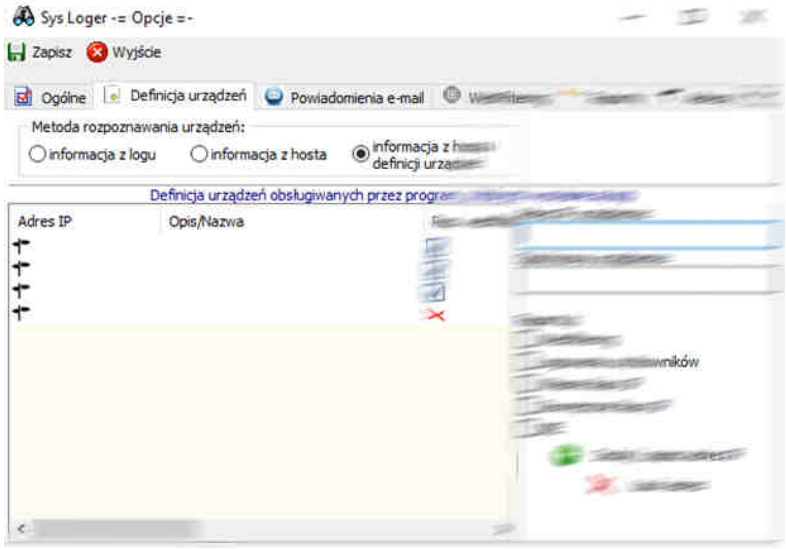
Zakładka Ogólne.

W zakładce Ogólne ustawiamy:

- zapis logów do pliku tekstowego wskazując katalog z logami oraz stałą nazwę pliku z logami. Do stałej nazwy pliku dodana zostanie część z datą dnia logu,
- ilość wpisów w oknie logu monitora,

(…)

Zakładka Definicja urządzeń.



W zakładce tej definiujemy listę urządzeń podając dodatkowe indywidualne cechy potrzebne do codziennego raportowania, tj.:

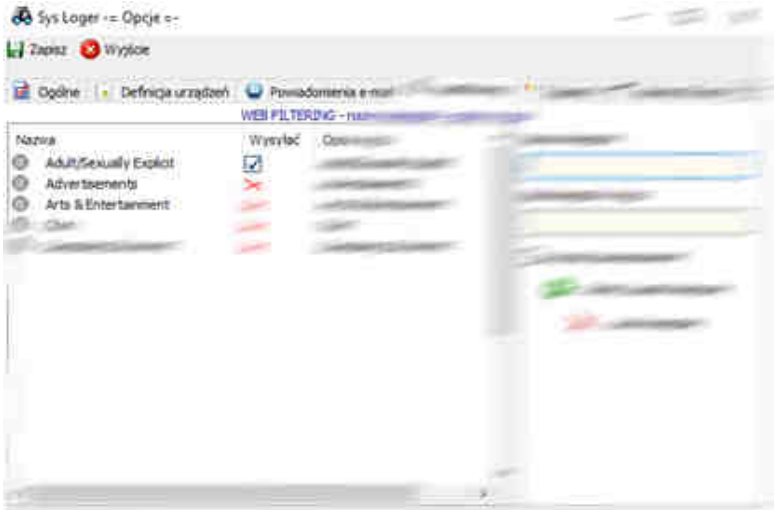
- webfilteringu,
- logowań użytkowników,
  (…)

Brak ustawienia raportowania indywidualnego przy urządzeniu oznaczać będzie jego pominięcie pomimo ustawienia parametrów ogólnych w zakładce: Raporty.

W ramach metody **rozpoznawania urządzeń** dostępne są trzy możliwości:

- **informacja z logu** – adres IP urządzenia przesyłającego pobierany jest z otrzymywanego logu (dla tej opcji możliwa jest sytuacja, że urządzenie będzie się identyfikowało własną wewnętrzną nazwą zamiast oczekiwanym adresem),
  (…)

Zakładka webfiltering.



W zakładce tej definiujemy webfiltering jaki jest stosowany na urządzeniu brzegowym. Ustawiamy tutaj również automatyczne informowanie o jej wstąpieniu.

Ustawienia webfilteringu są wykorzystywane przy generowaniu codziennych raportów, przypisanie raportu z webfilteringu do urządzenia dokonywane jest na etapie definiowania urządzenia w zakładce: Definicja urządzeń.

(…)