Zadania

0. Dostęp do panelu zarządzania

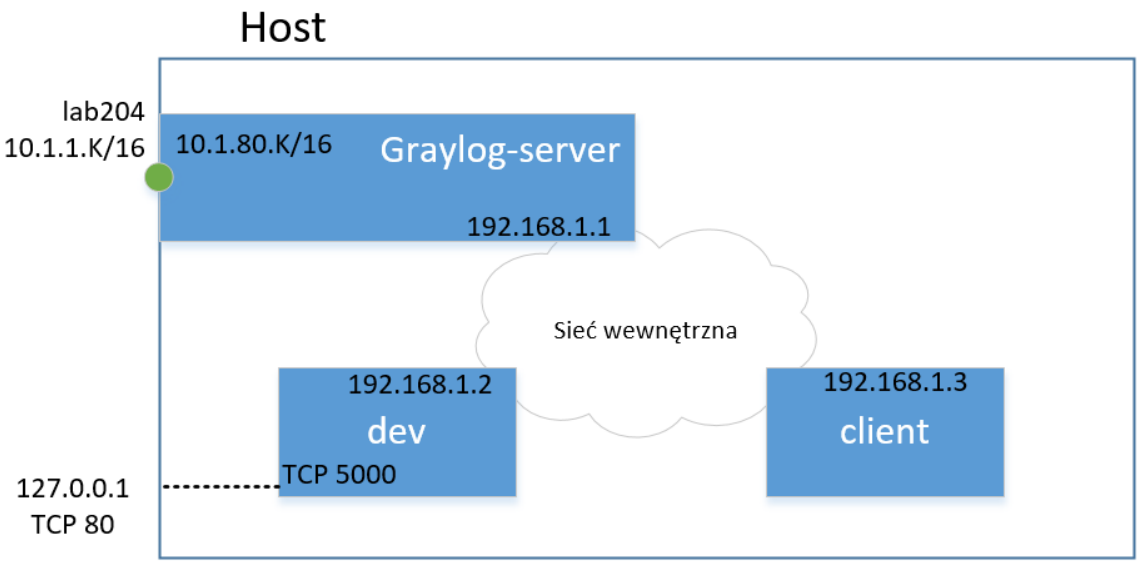
Na potrzeby ćwiczenia laboratoryjnego przygotowane zostało środowisko w postaci wirtualnych maszyn uruchamianych z poziomu systemu Vagrant.

Plik konfiguracyjny *Vagrantfile* środowiska znajduje się w katalogu d:/zbi2/. W pliku tym należy zmienić adres IP maszyny graylog, ustawiając go w wierszu:

graylog.vm.network "public_network", ip: "10.1.80.1", netmask:"255.0.0.0", bridge: "Intel(R) Ethernet Connection (7) I219-V"

Adres IP należy zmienić zgodnie ze schematem 10.1.80.K, gdzie K oznacza numer komputer. Modyfikacja ta pozwoli na dostęp do interfejsu zarządzania serwera Graylog przez skonfigurowany adres IP.

Pozostałe wirtualne maszyny nie wymagają dostosowywania konfiguracji do stanowiska pracy. Schemat środowiska został zaprezentowany został na poniższym rysunku.



Przed uruchomieniem środowiska niezbędne jest uruchomienie wiersza poleceń, przejście do katalogu d:/zbi2/ i załadowanie obrazów wzorcowych dla wykorzystywanych maszyn:

vagrant box add graylog-server graylog.box

vagrant box add graylog-dev dev.box

Następnie w celu uruchomienia środowiska należy wpisać polecenie: *vagrant up*. Dostęp od poszczególnych maszyn można uzyskać wpisując odpowiednio: *vagrant ssh graylog*, *vagrant ssh client*, *vagrant ssh dev*. W konsoli każdego systemu dostępne jest narzędzie tmux.

W pliku konfiguracyjnym serwera graylog (*/etc/graylog/server/server.conf*) należy ustawić adres IP 10.1.80.K w opcji `http_bind_address`, pozostawić port 9000 bez zmian oraz ponowanie uruchomić usługę graylog-server.

A. Monitorowanie danych z serwera i aplikacji webowej.

W maszynie *dev*, przygotowana została prosta aplikacja webowa. Jej pliki znajdują się katalogu /root/, odwzorowanym z katalogu d:/zbi2/dev_files/, z którego to można edytować pliki na poziomie systemu operacyjnego hosta.

Uruchomienie maszyny odbywa się poprzez polecenie: *bash run_demo_app*

Sama aplikacja znajduje się w pliku: *zbi_demo.py*. Dostęp do uruchomionej usługi odbywa się przez połączenie z adresem 127.0.0.1 komputera hosta.

A.1. W GUI serwera graylog skonfigurować nowe źródło danych GELF UDP.

A.2. W pliku zbi_demo.py skonfigurować serwer logowania graylog podając odpowiedni adres IP skonfigurowanego źródła w zad. A.1.

A.3. Dodać odpowiednie ekstraktory pozwalające na wyodrębnienie szczegółów pola żądania (request) oraz nagłówka (header) uzyskując szczegóły dotyczące kodu odpowiedzi oraz URL.

A.4. Skonfigurować kolejność procesorów zgodnie z poniższą listą wyłączać AWS Instance Name Lookup:

1. Message Filter Chain
2. Pipeline Processor
3. GeoIP Resolver
4. AWS Instance Name Lookup

A.5. Dodać strumienie wiadomości filtrując widomości z serwera www oraz aplikacji.

A.6. Zdefiniować reguły (Pipelines - Rules) pozwalające na przekształcenie typu danych pola określającego czas odpowiedzi na wartości liczbowe.

A.7. Przygotować wykres wartości średniej czasu odpowiedzi dla wybranego URL.

A.8. Przygotować w zakładce Dashboard tabelę prezentującą maksymalny czas odpowiedzi dla dostępnych URL.

A.9. Dodać alarm wywołany po wystąpieniu w ciągu minuty 5 błędów o kodzie 500.

Wyniki zaprezentować prowadzącemu.

B. Logowanie informacji o ruchu sieciowym

B.1. Skonfigurować na węzłach *dev* oraz *client* iptables tak aby pozwalały na logowanie informacji o ruchu wychodzącym UDP port docelowy 53 w syslog.

B.2. Skonfigurować nowe źródło danych RSYSLOG UDP w serwerze graylog. UWAGA: Należy zastosować niestandardowy numer portu powyżej numeru 1024, np. 5514.

B.3. Skonfigurować na maszynach *dev* oraz *client* klienta rsyslog, przekazującego wiadomości do serwera graylog.

B.4. Dodać ekstraktor GROK pozwalający na wyodrębnienie m.in. adresów IP i długości zapytania DNS dla logowanych wiadomości.

B.5. Dodać strumień wiadomości dla tego typu źródła.

B.6. Zdefiniować reguły pozwalające na przekształcenie typu danych pola określającego długość zapytania DNS na wartości liczbowe (nazwa pola zależy od reguły GROK).

B.7. Przygotować w zakładce Dashboard tabelę prezentującą adresy IP wykorzystywanych serwerów DNS, liczbę wiadomości oraz średni rozmiar wiadomości z ostatnich 5 minut.

B.8 Zestawić tunel IP-over-DNS wykorzystując polecenie:

iodine -f -r 10.1.2.203 test.com

B.9 Zaprezentować wyniki w przygotowanej tabeli dla generowanego ruchu w łączu tunelowanym (np. ping 172.16.0.1 -s 1000).

Zaprezentować wyniki prowadzącemu.