

Oprogramowanie zabezpieczające SO w tym skanery antywirusowe i profilaktyka antywirusowa.

Przed przystąpieniem do ćwiczenia sprawdź czy ustawienia maszyny wirtualnej z Windows



Polecane oprogramowania do ćwiczeń AVG_Protection_Free. Wybierz z Internetu lub urządzenia

Napędy optyczne, wybierz obraz dysku  oprogramowanie.iso .

Zadanie 1

Wykonaj kolejne czynności dla programu antywirusowego i antyspyware.

1.1 Instalacje programu do usuwania złośliwego oprogramowanie (szkodliwego kodu).

1.2 Aktualizacje (z folderu) baz programu do usuwania złośliwego oprogramowanie.

<https://support.avg.com/SupportArticleView?l=pl&urlname=How-to-update-AVG>

1.3 Skanowanie komputera i usuwanie złośliwego oprogramowanie.

Wirus testowy eicar pobierz z <http://2016.eicar.org/85-0-Download.html>

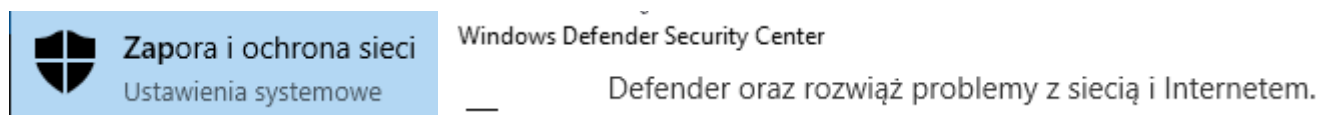
1.4 Włączenie ochrony rezydentnej (trybu monitora).

1.5 Włączenie automatycznych aktualizacji programu antywirusowego.

Zadanie 2

Wykonaj kolejne czynności dla konfiguracji zapory.

2.2 Włącz zaporę systemową. Ustaw zaporę, aby przepuszczała komunikacje programów Gadu-gadu, udostępnianie plików i drukarek, pulpitu zdalnego oraz ping.



[Zezwalaj aplikacji na dostęp przez zaporę](#)

Aby dodać, zmienić lub usunąć dozwolone aplikacje i porty, kliknij pozycję Zmień ustawienia.

Pulpit zdalny

Udostępnianie plików i drukarek

Zdalne zamykanie systemu

netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request"
protocol=icmpv4:8,any dir=in action=allow

```
c:\Windows\system32>netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol=icmpv4:8,any dir=in action=allow
```

Zapora Windows Defender Ustawienia zaawansowane

- Zapora Windows Defender z zał
- Reguły przychodzące
- Reguły wychodzące
- Reguły zabezpieczeń połączeń
- Monitorowanie

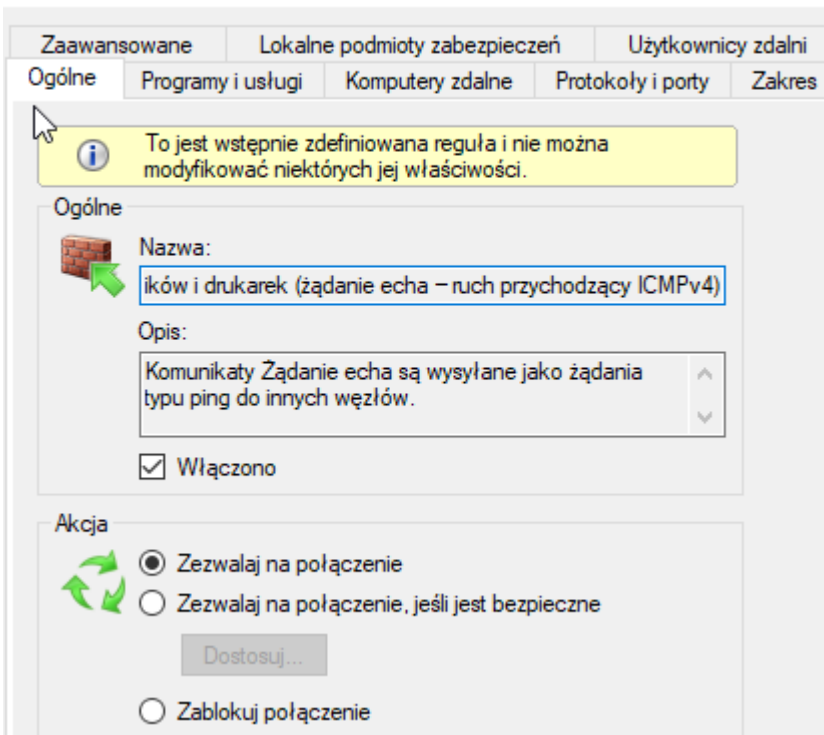
| Nazwa | Grupa |
|---|---------------------------------|
| Udostępnianie plików i drukarek (żądanie echa — ruch przychodzący ICMPv4) | Udostępnianie plików i drukarek |
| <input checked="" type="checkbox"/> Udostępnianie plików i drukarek (żądanie echa — ruch przychodzący ICMPv4) | Udostępnianie plików i drukarek |
| Udostępnianie plików i drukarek (żądanie echa — ruch przychodzący ICMPv6) | Udostępnianie plików i drukarek |

| Profil | Włączony | Akcja | Zastęp | Program | Adres lokalny | Adres zdalny |
|-----------|----------|-------|--------|---------|---------------|---------------|
| Prywatny | Nie | Zezwa | Nie | Dowolne | Dowolne | Podsieć lokal |
| Publiczny | Tak | Zezwa | Nie | Dowolne | Dowolne | Podsieć lokal |
| Domena | Nie | Zezwa | Nie | Dowolne | Dowolne | Dowolne |

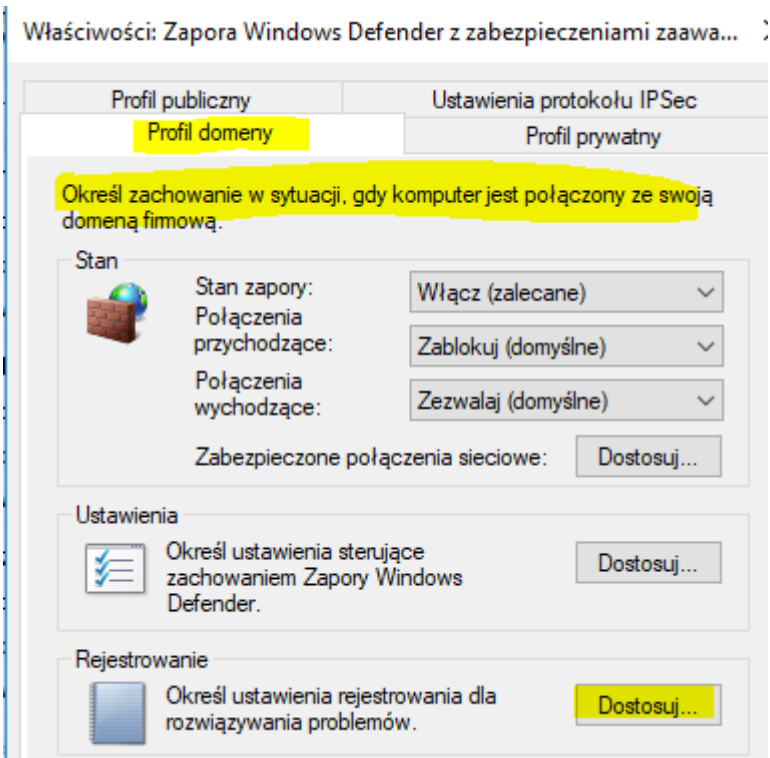
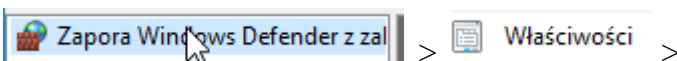
| Port lokalny | Port zdalny | Autoryzowani użytkownicy | Autoryzowane komputery | Autoryzowane lok |
|--------------|-------------|--------------------------|------------------------|------------------|
| Dowolne | Dowolne | Dowolne | Dowolne | Dowolne |
| Dowolne | Dowolne | Dowolne | Dowolne | Dowolne |
| Dowolne | Dowolne | Dowolne | Dowolne | Dowolne |

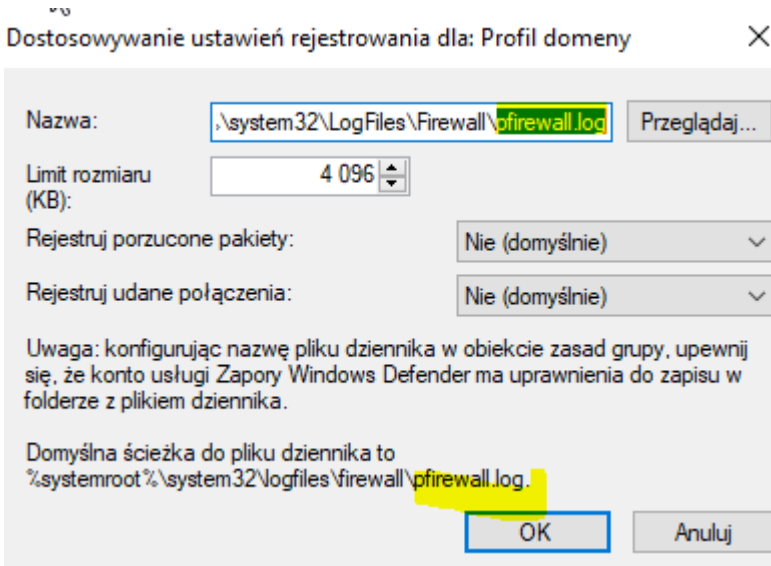
| Autoryzowane lokalne podmioty zabezpieczeń | Właściciel użytkownika lokalnego | Pakiet aplikacji |
|--|----------------------------------|------------------|
| Dowolne | Dowolne | Dowolne |
| Dowolne | Dowolne | Dowolne |
| Dowolne | Dowolne | Dowolne |
| Dowolne | Dowolne | Dowolne |

Właściwości: Udostępnianie plików i drukarek (żądanie echa — ruch przy... X

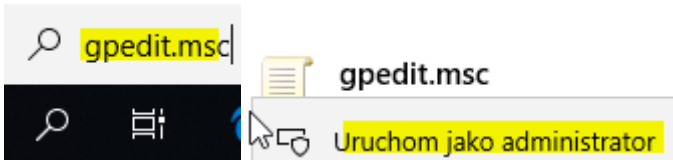


2.3 Zapisz lokalizację domyślną. Ustaw logowanie porzuconych pakietów zapory do pliku c:\zapora.log



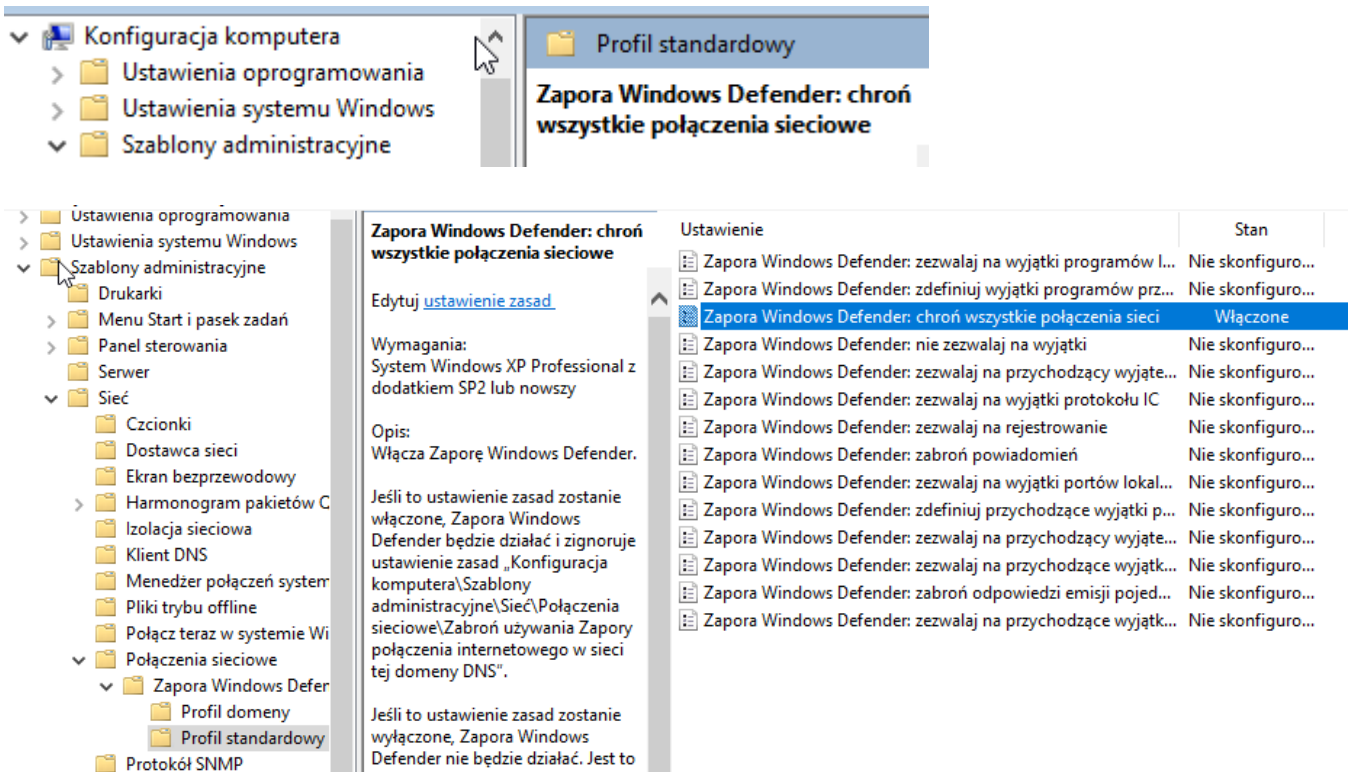


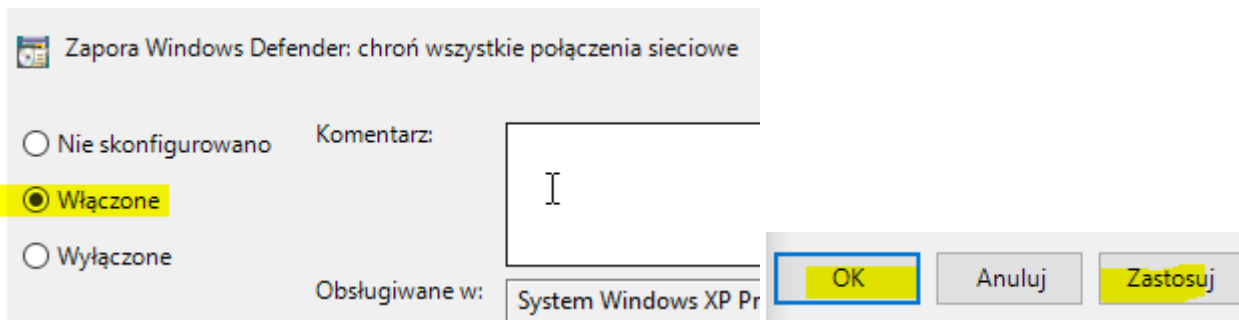
2.4 Ustaw włączenie zapory w zasadach grup (gpedit.msc)



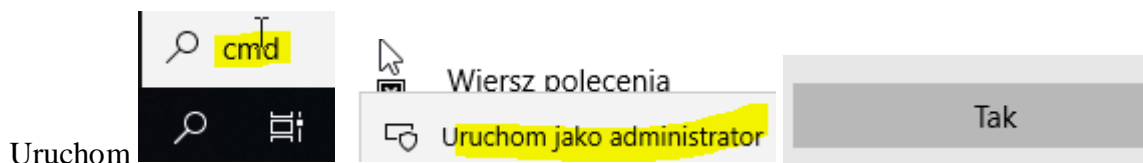
Konfiguracja Komputera → Szablony administracyjne → Sieć → Połączenia sieciowe → Zapora Windows Defender → Profil standardowy: chroń wszystkie połączenia sieciowe.

Edytuj ustawienie i zmień jego status na **włączony**. Zapisz zmiany poprzez użycie przycisku **Zastosuj**.





Wkonaj gpupdate /force w celu odświeżenia zasad



```
C:\> Administrator: Wiersz poleceń
Microsoft Windows [Version 10.0.17134.1]
(c) 2018 Microsoft Corporation. Wszelkie prawa zastrzeżone.

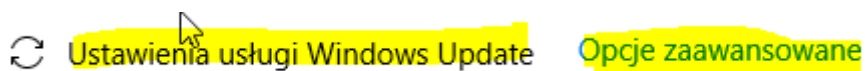
C:\Windows\system32>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

Zadanie 3

Zapisz w zeszycie kolejne czynności, które należy wykonać w celu

1. Ustawienia systemu operacyjnego w tryb automatycznych aktualizacji.



Opcje aktualizacji

Włącz aktualizacje innych produktów firmy Microsoft, gdy aktualizuję system Windows.

Wyłączone

Automatycznie pobieraj aktualizacje, nawet za pośrednictwem taryfowych połączeń danych (mogą być naliczane opłaty)

Wyłączone

Wyświetlimy przypomnienie, gdy będziemy chcieli wykonać ponowne uruchomienie. Jeśli chcesz otrzymywać więcej powiadomień dotyczących ponownego uruchomienia, włącz to ustawienie.

Wyłączone

Wstrzymaj aktualizacje

Tymczasowo wstrzymaj instalowanie aktualizacji na tym urządzeniu na maksymalnie 35 dni. Gdy aktualizacje zostaną wznowione, konieczne będzie pobranie najnowszych aktualizacji na to urządzenie, aby można było ponownie wstrzymać aktualizacje.

Wyłączone

Wstrzymanie teraz spowoduje wstrzymanie aktualizacji do 23.04.2019

2. Wyjaśnij czym różnią się poszczególne opcje.

Określ, kiedy mają być instalowane aplikacje

Wybierz poziom gotowości gałęzi, aby ustalić, kiedy są instalowane aktualizacje funkcji. "Półroczny kanał (kierowany)" informuje o dostępności aktualizacji dla większości osób, a "półroczny kanał" oznacza, że aktualizacja jest gotowa do powszechnego użycia w organizacjach.

Półroczny kanał (kierowany) ▾

Aktualizacja funkcji zawiera nowe możliwości i ulepszenia. Można ją odroczyć na następującą liczbę dni:

0 ▾

Aktualizacja dotycząca jakości zawiera ulepszenia w zakresie zabezpieczeń. Można ją odroczyć na następującą liczbę dni:

0 ▾

Optimalizacja dostarczania

[Ustawienia prywatności](#)

Uwaga: usługa Windows Update może się aktualizować automatycznie, zanim będzie wyszukiwać inne aktualizacje.

Skonfiguruj automatyczną konfigurację urządzenia po aktualizacji w sekcji Prywatność [Opcje logowania](#)

🏠 Optymalizacja dostarczania

Optymalizacja dostarczania Windows Update umożliwia szybką i niezawodną aktualizację systemu Windows i aplikacji ze sklepu Store oraz innych produktów firmy Microsoft.

Zezwalaj na pobieranie plików z innych komputerów

W przypadku niestabilnego łącza internetowego lub aktualizowania kilku urządzeń, zaznaczenie opcji pobierania z innych komputerów pozwoli przyspieszyć proces.

Włączenie tej funkcji może spowodować wysyłanie z komputera części pobranych aktualizacji i aplikacji systemu Windows do, w zależności od opcji zaznaczonych poniżej, komputerów w sieci lokalnej lub Internecie. Jeśli korzystasz z połączenia taryfowego, komputer nie będzie wysyłał treści do innych komputerów przez Internet.

[Dowiedz się więcej](#)

Zezwalaj na pobieranie plików z innych komputerów

Włączone

Komputery w mojej sieci lokalnej

Komputery w mojej sieci lokalnej i w Internecie

Opcje zaawansowane

[Monitorowanie aktywności](#)

Opcje zaawansowane

Domyślnie dynamicznie optymalizujemy przepustowość, której urządzenie używa w celu pobierania i przekazywania aktualizacji systemu Windows i aplikacji oraz innych produktów firmy Microsoft. Jeśli martwisz się zużyciem danych, możesz ustawić określony limit.

Ustawienia pobierania

Ogranicz poziom przepustowości wykorzystywany do pobierania aktualizacji w tle

45%

Ogranicz poziom przepustowości wykorzystywany do pobierania aktualizacji na pierwszym planie

90%

Ustawienia wysyłania

Ogranicz poziom przepustowości wykorzystywany do przesyłania aktualizacji do innych komputerów przez Internet

50%

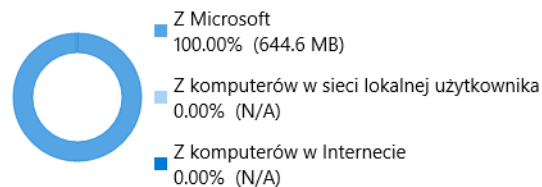
Miesięczny limit wysyłania danych

500 GB

Monitorowanie aktywności

Statystyka pobierania

Od 01.03.2019

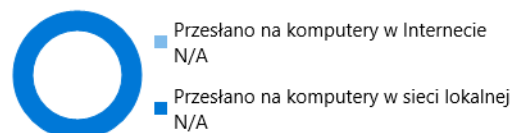


Średnia szybkość pobierania (zainicjowane przez użytkownika): N/A

Średnia szybkość pobierania (w tle): 10.7 Mbps

Statystyka wysyłania

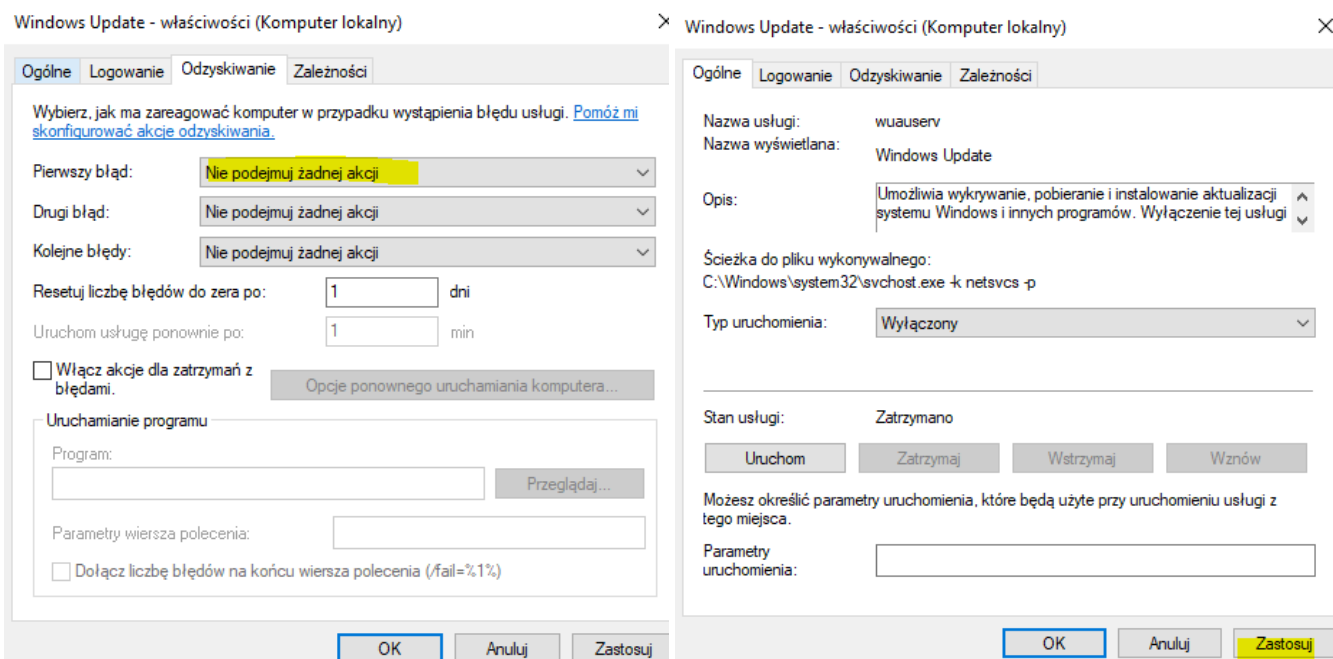
Od 01.03.2019



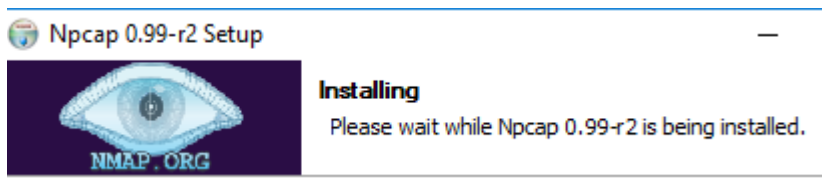
3. W celach sprawnego wykonywania ćwiczeń pozostaw ustawienie

The screenshot shows the Windows Services console with the 'Windows Update' service selected. The 'Zatrzymaj usługę' button is highlighted in blue. A dialog box titled 'Sterowanie usługą' is open, showing a progress bar and the 'Zatrzymaj' button highlighted in blue. The dialog box also contains the text 'Windows próbuje zatrzymać następującą usługę na Komputer lokalny...' and 'Zamknij' button.

Efekt

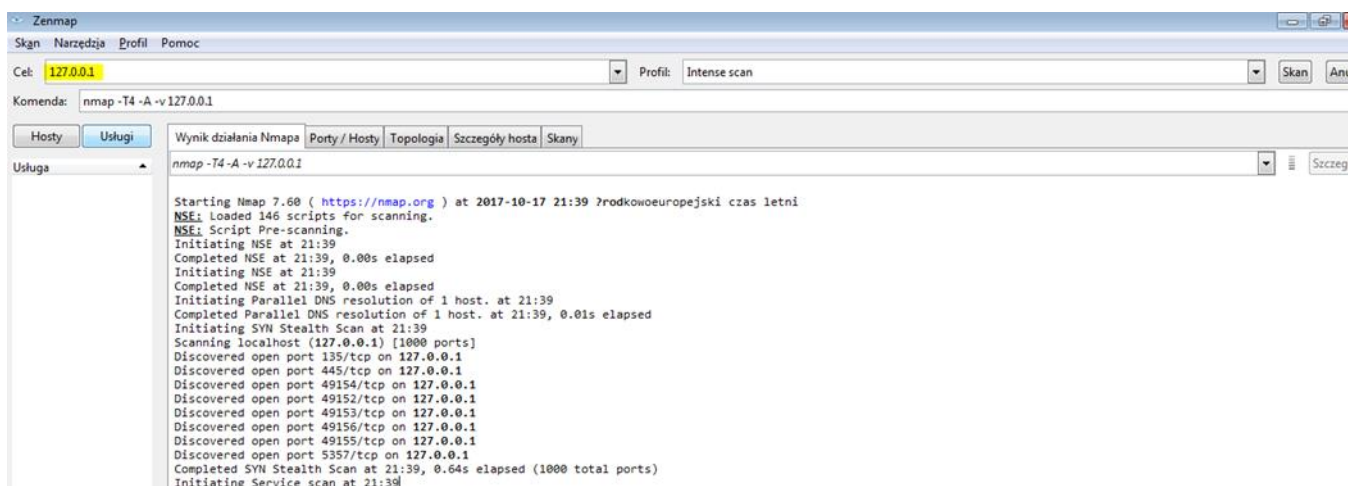


4. Zainstaluj program nmap z



4.1a Sprawdź za pomocą programu nmap otwarte porty na komputerze. Cel: **127.0.0.1**

4.1b Opisz jakie porty są otwarte i jakie w tych portach pracują usługi.



5. Ustawienia właściwej konfigurację przeglądarki programów pracujących w sieciach np. Internecie (wybierz dowolną) dodaj Adblock.