Uniwersytet WSB Merito w Poznaniu

Wydział Finansów i Bankowości

Studia stacjonarne I stopnia – Informatyka

**Sprawozdanie**

**z wykonania ćwiczenia laboratoryjnego**

Przedmiot: **Podstawy ochrony danych**

Grupa: **K32**

Rok akad.: **2023/2024**

Prowadzący: dr inż. Izabela Janicka-Lipska

**Ćwiczenie 01**

Temat: **Programy szkodliwe**

Student: **Grzegorz Olejniczak**

Data wykonania: **28.09.2024r.**

1. Cel ćwiczenia  
Zapora sieciowa (ang. firewall) to narzędzie zabezpieczające, które kontroluje i monitoruje ruch sieciowy w celu ochrony systemu przed nieautoryzowanym dostępem oraz zagrożeniami z zewnątrz. Celem ćwiczenia było zbadanie funkcjonalności zapory sieciowej oraz jej konfiguracji w celu blokowania i zezwalania na określone połączenia sieciowe.

1. Cel ćwiczenia  
Zapora sieciowa (ang. firewall) to narzędzie zabezpieczające, które kontroluje i monitoruje ruch sieciowy w celu ochrony systemu przed nieautoryzowanym dostępem oraz zagrożeniami z zewnątrz. Celem ćwiczenia było zbadanie funkcjonalności zapory sieciowej oraz jej konfiguracji w celu blokowania i zezwalania na określone połączenia sieciowe.

2. Stosowane aplikacje  
Ćwiczenie wykonano korzystając z aplikacji:  
- Zapora systemu Windows z zaawansowanym zabezpieczeniami  
- Wireshark do analizy ruchu sieciowego  
- VirtualBox w celu symulacji różnych scenariuszy sieciowych

Ćwiczenie wykonano korzystając z aplikacji:

1. Nazwa programu
2. …
3. 3. Wykonane badania  
   W ramach ćwiczeń skonfigurowano zaporę sieciową w systemie Windows, definiując reguły blokowania oraz zezwalania na ruch sieciowy. Testy zostały przeprowadzone na ruchu sieciowym symulowanym przez VirtualBox i analizowanym w Wireshark. Kroki wykonania:  
   1. Utworzenie reguły blokującej połączenia na określony port  
   2. Testowanie połączenia z użyciem narzędzia ping i Wireshark  
   3. Utworzenie reguły zezwalającej na ruch HTTP i analiza pakietów w Wireshark.  
     
   Poniżej znajdują się wycinki z ekranów dokumentujące przeprowadzone testy:

3. Wykonane badania  
W ramach ćwiczeń skonfigurowano zaporę sieciową w systemie Windows, definiując reguły blokowania oraz zezwalania na ruch sieciowy. Testy zostały przeprowadzone na ruchu sieciowym symulowanym przez VirtualBox i analizowanym w Wireshark. Kroki wykonania:  
1. Utworzenie reguły blokującej połączenia na określony port  
2. Testowanie połączenia z użyciem narzędzia ping i Wireshark  
3. Utworzenie reguły zezwalającej na ruch HTTP i analiza pakietów w Wireshark.  
  
Poniżej znajdują się wycinki z ekranów dokumentujące przeprowadzone testy:

…

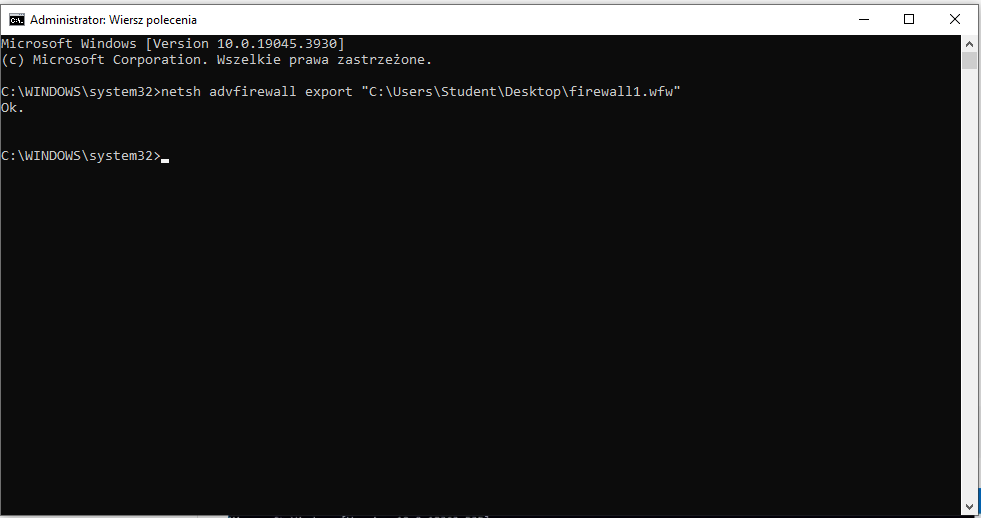
1. **Uzyskane rezultaty**

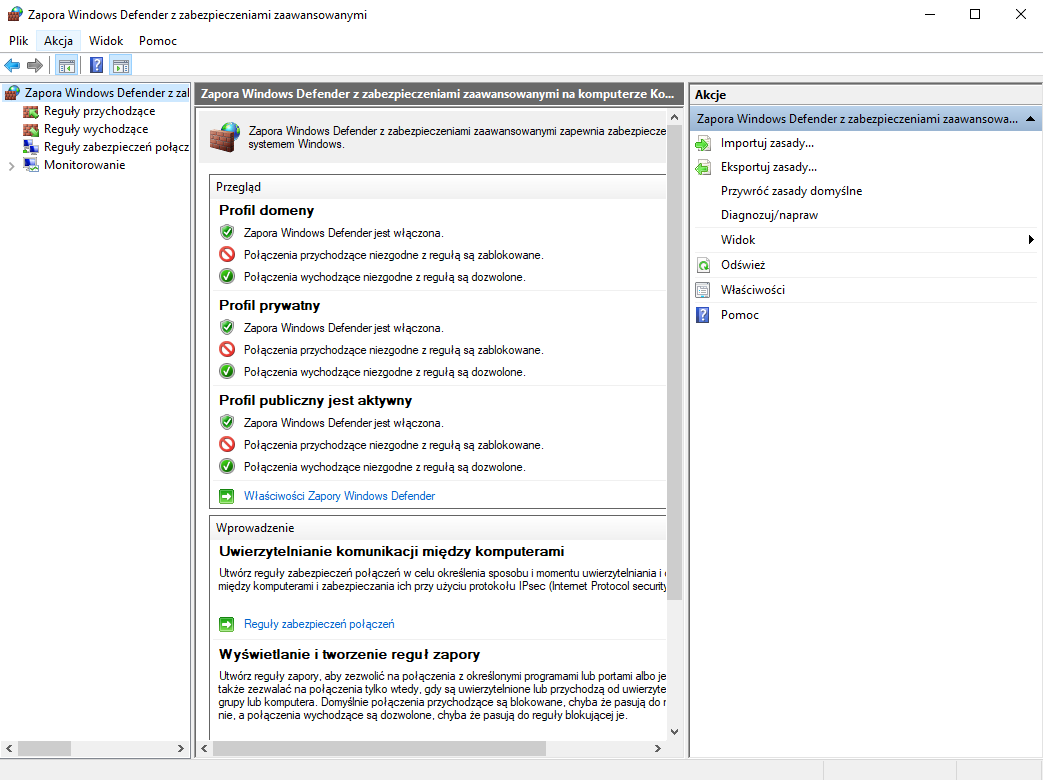
*Tutaj umieszczamy informacje jak „to” zostało zrobione czyli screeny z opisem, wykonane obliczenia, zastosowane narzędzia ...*

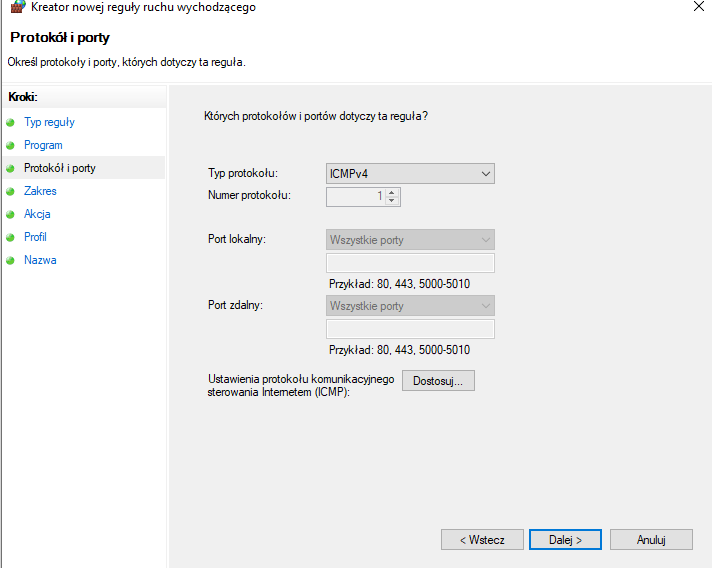
...

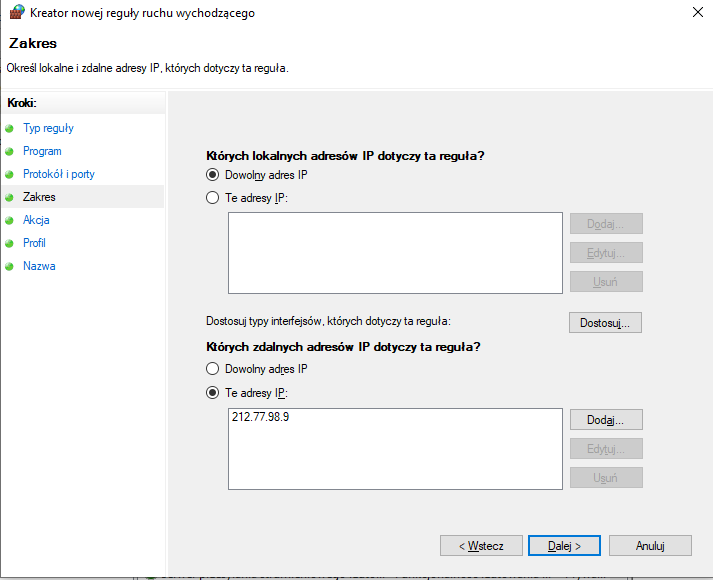
5. Wnioski i uwagi  
Ćwiczenie pozwoliło zrozumieć, jak istotną rolę pełni zapora sieciowa w zapewnianiu bezpieczeństwa sieci. Pozwoliło również zapoznać się z narzędziami do monitorowania ruchu sieciowego, takimi jak Wireshark. Praktyczna konfiguracja reguł zapory sieciowej nauczyła precyzyjnego kontrolowania dostępu do zasobów sieciowych, co może być wykorzystane w przyszłej pracy zawodowej.

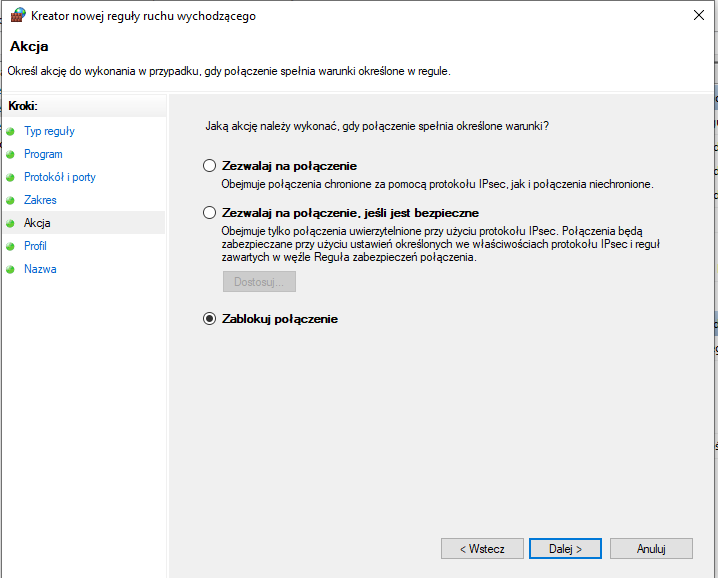
5. Wnioski i uwagi  
Ćwiczenie pozwoliło zrozumieć, jak istotną rolę pełni zapora sieciowa w zapewnianiu bezpieczeństwa sieci. Pozwoliło również zapoznać się z narzędziami do monitorowania ruchu sieciowego, takimi jak Wireshark. Praktyczna konfiguracja reguł zapory sieciowej nauczyła precyzyjnego kontrolowania dostępu do zasobów sieciowych, co może być wykorzystane w przyszłej pracy zawodowej.

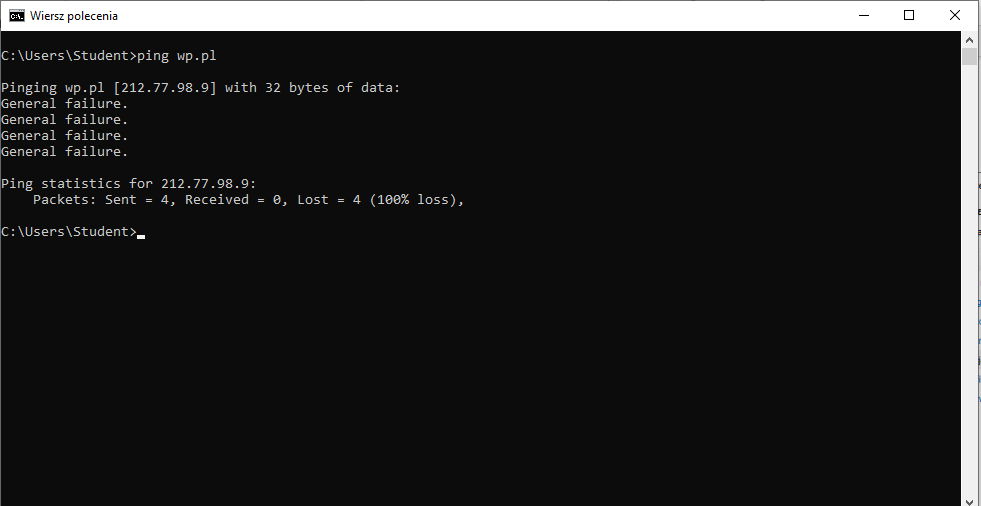
... 

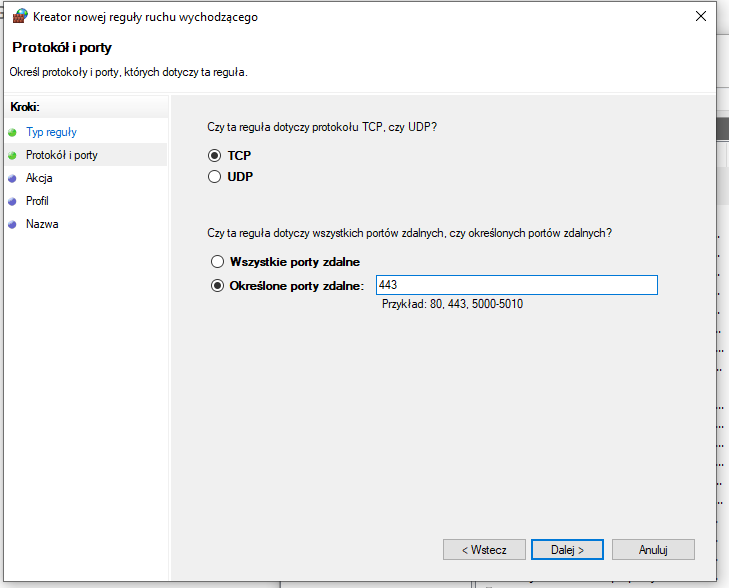


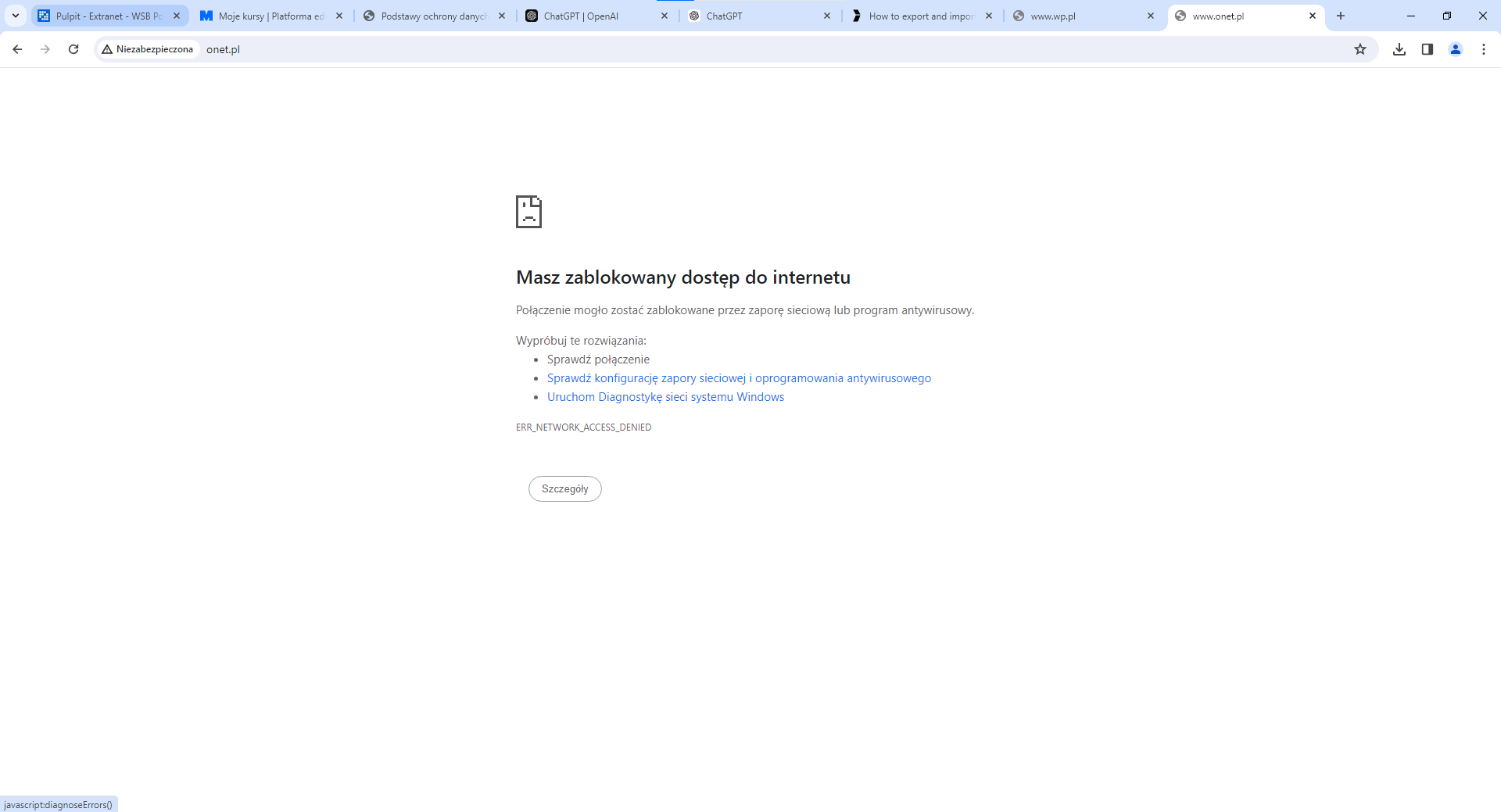


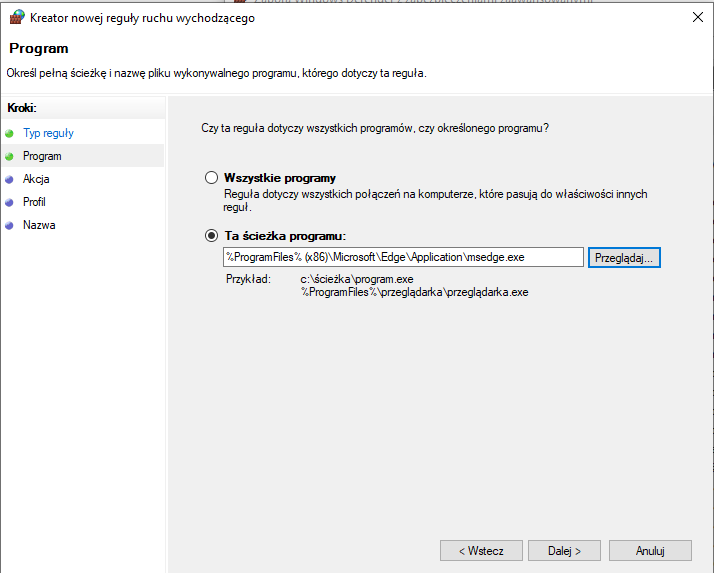


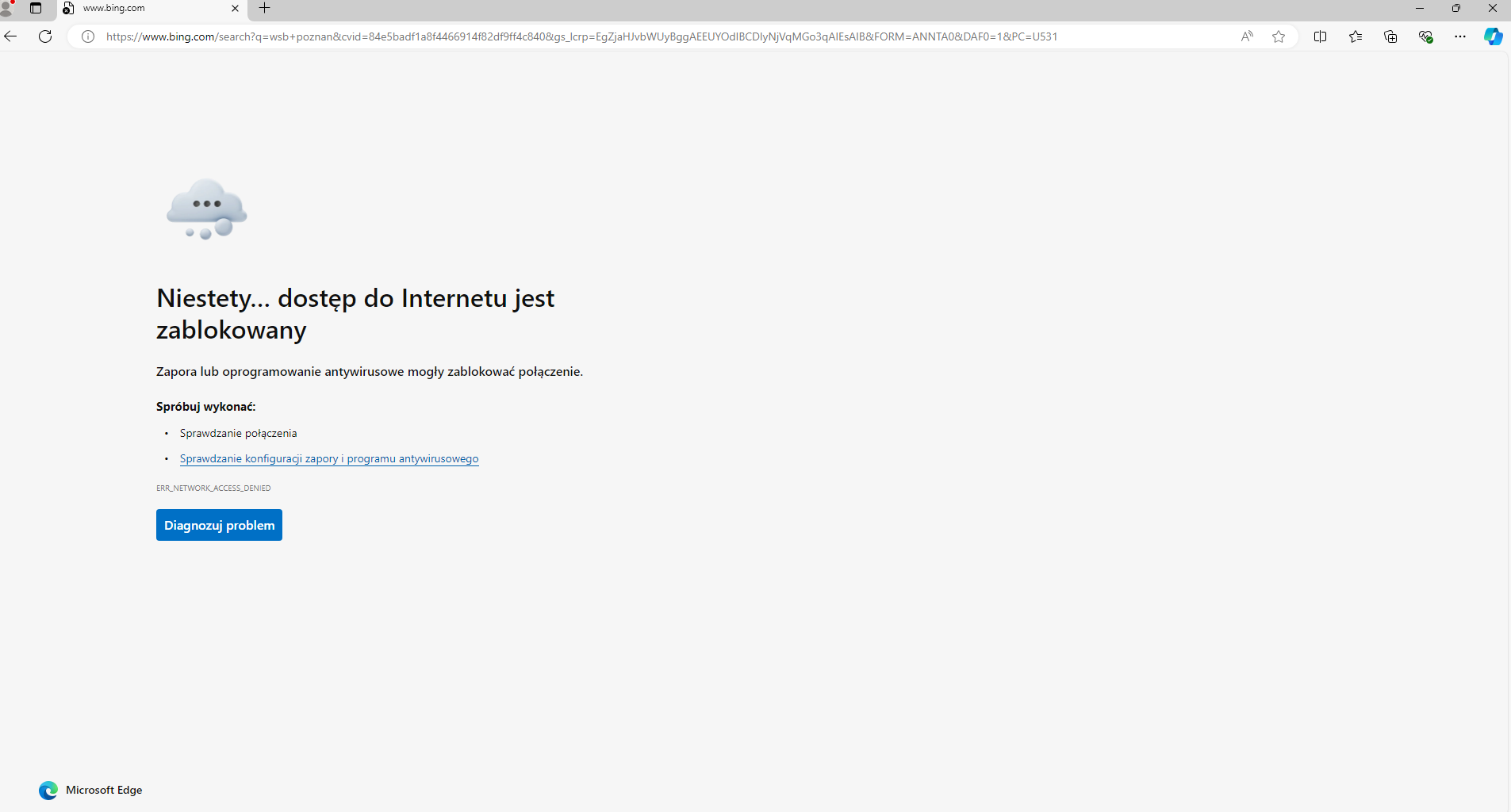


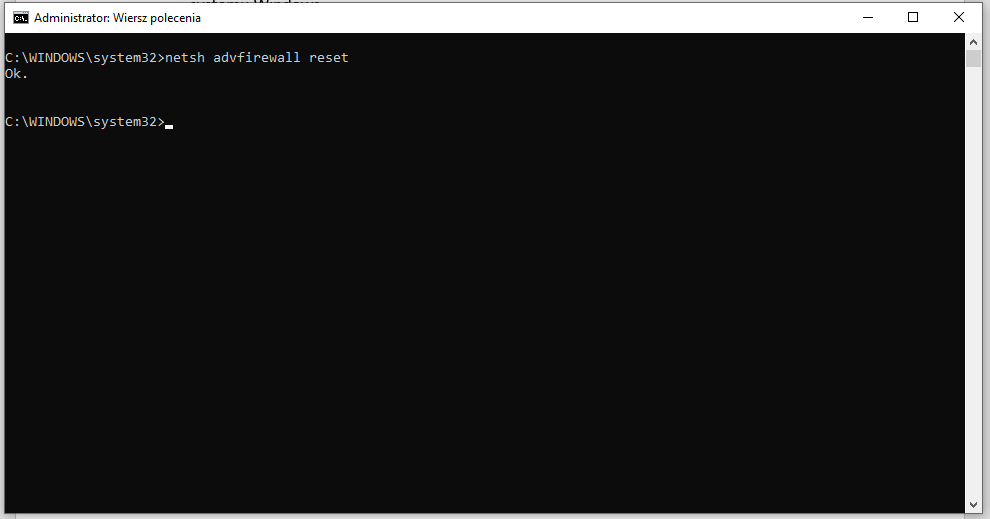












**6. Literatura**

Należy wpisać portale internetowe, pozycje literatury (książki, artykuły naukowe z czasopism, artykuły naukowe konferencyjne, normy, *white papers* – podając pełne dane bibliograficzne; **nie cytujemy haseł z Wikipedii!**), które służyły do przygotowania się do ćwiczenia i/lub były pomocne przy wykonywaniu ćwiczenia, np.:

1. …

…

Uwaga:

Sprawozdanie należy przesłać w pliku

POD-nr-nazwisko-imię.pdf

gdzie:

nr= 01, 02, …, 12 oznacza numer ćwiczenia,

nazwisko-imię jest nazwiskiem i imieniem studenta wykonującego ćwiczenie,

umieszczając je na platformie Moodle.

Przed zapisaniem pliku   
w formacie **pdf**   
tę stronę **należy usunąć**.