Bezpieczeństwo sieci komputerowych Temat: Firewall sieci domowej

Data: 30/04/2022 Ewa Namysł Informatyka stosowana, III rok

1. Opis i cel zadania:

Celem zadania jest opisanie w jaki sposób skonfigurowany jest firewall na urządzeniu sieciowym oraz komputerze w sieci domowej.

2. Zapora sprzętowa modemu Wi-Fi w trybie routera:

Zapora firewall IPv4	
Zapora sieciowa	✓ Włączony
Blokuj fragmentowane pakiety IP	☐ Włączony
Wykrywanie skanowania portów	✓ Włączony
Wykrywanie ataków typu IP flood	✓ Włączony
Wykrywanie ataków typu ICMP flood	✓ Włączony
Zakres dla wykrywania ataku typu ICMP flood	15

Firewall jest włączony, co jest domyślną konfiguracją dla tego dostawcy internetu. Ponadto włączone są opcje, które pozwalają wykrywać skanowanie portów, IP flood oraz ICMP flood.

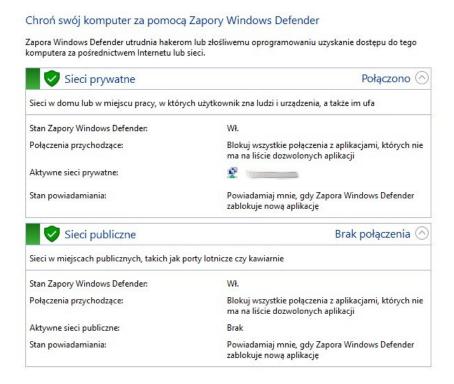
Pierwsza z tych opcji sprawdza czy do sieci przesyłane są pakiety, mające na celu ustalenie jakie porty są dostępne. Otwarte porte mogą być wykorzystane do złamania zabezpieczeń systemu.

Opcje wykrywania ataków typu IP flood oraz ICMP flood związane są z atakami typu denial of service. Pakiety przesyłane w szybkim czasie mogą przeciążyć łącze i uniemożliwić normalną pracę lub ograniczyć dostępność.

Opcją, która nie jest włączona to blokowanie fragmentacji pakietów IP. Może to narażać sieć na ataki, które opierają się o fragmentację pakietów i denial of service.

Z dodatkowych opcji bezpieczeństwa, strefa DMZ nie została włączona, ponieważ żadne z urządzeń z sieci nie jest wykorzystywane jako serwer dostępny dla sieci zewnętrznej.

3. Zapora sieciowa systemu Windows:



Firewall jest włączony z domyślną konfiguracją zarówno dla sieci prywatnych, jak i publicznych. Zapora informuje o blokowaniu nowych aplikacji, ponadto blokuje połączenia z aplikacjami, które nie są na liście dozwolonych.

W zaawansowanych ustawieniach można podejrzeć reguły przychodzące i wychodzące, znajdują się tam głównie aplikacje i programy dopuszczone do łączenia się z siecią.



Cztery pierwsze otwarte porty na liście wykorzystywane są przez usługi Windowsa. Dwa kolejne dla procesów o PID 4520 to porty wykorzystywane przez tablet graficzny. Dalej pojawiają się porty zarówno dla usług Windowsa, buforu wydruku, jak i aplikacji m.in. przeglądarki internetowej.

