

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	<input checked="" type="checkbox"/> Włączony
Blokuj fragmentowane pakiety IP	<input type="checkbox"/> Włączony
Wykrywanie skanowania portów	<input checked="" type="checkbox"/> Włączony
Wykrywanie ataków typu IP flood	<input checked="" type="checkbox"/> Włączony
Wykrywanie ataków typu ICMP flood	<input checked="" type="checkbox"/> Włączony
Zakres dla wykrywania ataku typu ICMP flood	<input type="text" value="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 porty 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:

Chroń swój komputer za pomocą Zapory Windows Defender

Zapora Windows Defender utrudnia hakerom lub złośliwemu oprogramowaniu uzyskanie dostępu do tego komputera za pośrednictwem Internetu lub sieci.

 Sieci prywatne

Połączono 

Sieci w domu lub w miejscu pracy, w których użytkownik zna ludzi i urządzenia, a także im ufa



Stan Zapory Windows Defender:

Wł.

Połączenia przychodzące:


Blokuj wszystkie połączenia z aplikacjami, których nie ma na liście dozwolonych aplikacji


Aktywne sieci prywatne:

Stan powiadamiania:

Powiadamiam mnie, gdy Zapora Windows Defender zablokuje nową aplikację

 Sieci publiczne

Brak połączenia 

Sieci w miejscach publicznych, takich jak porty lotnicze czy kawiarnie

Stan Zapory Windows Defender:

Wł.

Połączenia przychodzące:

Blokuj wszystkie połączenia z aplikacjami, których nie ma na liście dozwolonych aplikacji

Aktywne sieci publiczne:

Brak

Stan powiadamiania:

Powiadamiam mnie, gdy Zapora Windows Defender zablokuje nową aplikację

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.

Reguły przychodzące				
Nazwa	Grupa	Profil	Wł...	Akcja
 Android Studio		Prywatny	Tak	Zezwalaj

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.

```
Administrator: Wiersz polecenia
C:\Windows\system32>netstat -aon

Active Connections

Proto Local Address           Foreign Address         State       PID
TCP   0.0.0.0:135              0.0.0.0:0               LISTENING   468
TCP   0.0.0.0:445              0.0.0.0:0               LISTENING   4
TCP   0.0.0.0:5040             0.0.0.0:0               LISTENING   7468
TCP   0.0.0.0:5357             0.0.0.0:0               LISTENING   4
TCP   0.0.0.0:23130            0.0.0.0:0               LISTENING   4520
TCP   0.0.0.0:23131            0.0.0.0:0               LISTENING   4520
TCP   0.0.0.0:49664            0.0.0.0:0               LISTENING   784
TCP   0.0.0.0:49665            0.0.0.0:0               LISTENING   680
TCP   0.0.0.0:49666            0.0.0.0:0               LISTENING   1592
TCP   0.0.0.0:49667            0.0.0.0:0               LISTENING   2004
TCP   0.0.0.0:49668            0.0.0.0:0               LISTENING   3412
TCP   0.0.0.0:49669            0.0.0.0:0               LISTENING   752
TCP   0.0.0.0:52890            0.0.0.0:0               LISTENING   9388
TCP   0.0.0.0:57621            0.0.0.0:0               LISTENING   9388
TCP   127.0.0.1:6463           0.0.0.0:0               LISTENING   5536
TCP   127.0.0.1:55749          127.0.0.1:65001         ESTABLISHED 14164
TCP   127.0.0.1:61770          127.0.0.1:61959         ESTABLISHED 16780
TCP   127.0.0.1:61959          0.0.0.0:0               LISTENING   17304
TCP   127.0.0.1:61959          127.0.0.1:61770         ESTABLISHED 17304
TCP   127.0.0.1:65001          0.0.0.0:0               LISTENING   14164
TCP   127.0.0.1:65001          127.0.0.1:55749         ESTABLISHED 14164
```