A black background with red text

Description automatically generated

***IT381 Zaštita i bezbednost informacija***

***Domaći zadatak br. 12***

***Ime i prezime: Jovan Pavkovic***

***Broj indeksa: 4442***

**Tekst zadataka**

Istražiti na internetu windows zaštitni zid i zatim implementirati tri pravila po izboru u windows-u 7,8 ili 10.

**Rešenje zadataka**

* Windows zaštitni zid (Windows firewall) je bezbednosna funkcija koja pomaže u zaštiti vašeg uređaja filtriranjem mrežnog saobraćaja koji ulazi i izlazi na vaš uređaj.
* Ovaj saobraćaj se može filtrirati na osnovu nekoliko kriterijuma, uključujući izvornu i odredišnu IP adresu, IP protokol ili broj izvornog i odredišnog porta.
* Windows zaštitni zid se može konfigurisati da blokira ili dozvoli mrežni saobraćaj na osnovu usluga i aplikacija koje su instalirane na vašem uređaju. Ovo vam omogućava da ograničite mrežni saobraćaj samo na one aplikacije i usluge kojima je izričito dozvoljeno da komuniciraju na mreži.
* Windows zaštitni zid je zaštitni zid zasnovan na hostu koji je uključen u operativni sistem i podrazumevano omogućen u svim izdanjima Windows-a.
* Windows zaštitni zid podržava bezbednost Internet protokola (IPsec), koji možete da koristite da zahtevate potvrdu identiteta sa bilo kog uređaja koji pokušava da komunicira sa vašim uređajem.
* Kada je potrebna potvrda autentičnosti, uređaji koji ne mogu da budu potvrđeni kao pouzdani uređaji ne mogu da komuniciraju sa vašim uređajem.
* Možete da koristite IPsec da biste zahtevali da određeni mrežni saobraćaj bude šifrovan kako biste sprečili da ga čitaju analizatori mrežnih paketa koje bi zlonamerni korisnik mogao da poveže sa mrežom. Windows zaštitni zid takođe radi sa svešću o mrežnoj lokaciji tako da može da primeni bezbednosna podešavanja koja odgovaraju tipovima mreža na koje je uređaj povezan.
* Na primer, Windows zaštitni zid može da primeni profil javne mreže kada je uređaj povezan na vi-fi kafića i profil privatne mreže kada je uređaj povezan na kućnu mrežu. Ovo vam omogućava da primenite restriktivnija podešavanja na javne mreže kako biste zaštitili svoj uređaj.
* Sledi prikaz informacija o tome kako je moguće podesiti pravila u Windows zaštitnom zidu na Windows 7, 8 ili 10.
* Ono što treba imati na umu jeste da se procedure mogu neznatno razlikovati u zavisnosti od verzije operativnog sistema Windows koja se koristiti.
* Windows 7:

1. Otvorite "Control Panel" i odaberite "System and Security".
2. Kliknite na "Windows Firewall".
3. Na levoj strani, odaberite "Advanced settings".
4. U prozoru koji se otvori, kliknite na "Inbound Rules" ili "Outbound Rules", zavisno o tome želite li kontrolisati dolazne ili odlazne veze.
5. Kliknite na "New Rule..." kako biste dodali novo pravilo.
6. Sledite uputstva čarobnjaka (wizzard) za postavljanje pravila, birajući tip pravila (Program, Port, itd.) i specificirajući uslove i akcije.

* Windows 8 i 10:

1. Desnim klikom miša kliknite na "Start" i odaberite "Control Panel" (Windows 8) ili "Windows PowerShell (Admin)" (Windows 10) kako biste otvorili PowerShell sa administratorskim privilegijama.
2. U PowerShell-u upišite wf.msc i pritisnite Enter kako biste otvorili Windows Firewall with Advanced Security.
3. Sledite korake 4-6 vezane za Windows 7.
4. Nakon što otvorite "Advanced settings" ili "Windows Firewall with Advanced Security", sledite uputstva čarobnjaka za dodavanje novog pravila. Odaberite tip pravila, specificirajte uslove (poput programa, portova ili IP adresa) i odredite akcije (blokiranje, dopuštanje, itd.).