УДК 004.942

ДОСЛІДЖЕННЯ ШВИДКОСТІ ПЕРЕДАЧІ ДАНИХ VPN З'ЄДНАНЬ ПРИ РІЗНИХ ТОПОЛОГІЯХ МЕРЕЖ

Э.М. Мамєдов[1], *О.О. Водка[2]*

[1] *магістрант кафедри ДММ, НТУ «ХПІ», Харків, Україна*

[2] *доцент кафедри ДММ, канд. техн. наук, НТУ «ХПІ», Харків, Україна mamiedov.elman.mo@gmail.com*

Щодня мільйони людей користуються інтернетом при цьому навіть не замислюються про те, що за всіма їхніми діями стежать сторонні люди (провайдер, місто, країна і можливо навіть зловмисники). Інтернет став грати дуже велику річ в наших теперішніх життях і реалії такі, що навіть те чим ми користуємося віддаючи за це гроші не надає нам 100% гранати того, що за нами не спостерігають під час наших пригод в ньому. Особливо небезпечними є безкоштовні точки роздачі інтернету з'єднання яким ми підключаємося з метою економії трафіку на мобільному телефоні.

Зміна IP - адреси не є вичерпним засобом захисту в сучасному світі[2]. У сучасному світі виявлення користувача відбувається за багатьма параметрами. Ідентифікатори заліза, відбитки браузера і багато-багато іншого. Виходячи з цих міркувань, на хостовій системі не повинно бути встановлене нічого стороннього. Таким чином ми захистимо себе від троянських коней, які ховаючись під більш-менш пристойними намірами, починають відправляти розробникам занадто багато даних.

В ході виконання роботи були створені власні VPN тунелі завдяки яким ми змогли приховувати своє знаходження в інтернеті від провайдера та інших людей. Тунелі були налаштовані на різних рівнях використовування, тобто за технологіями: VPN-Chain та VPN-namespace. Різні тунелі дозволяють нам керувати потоком даних які бачить провайдер та інші люди хто має намір спостерігати за нами через нашу IP – адресу. VPN-Chain – технологія за якою наш потік даних передається через ланцюжки VPN тунелів, доки не буде застосован останній, інакше кажучи, ми підключаємося до декількох тунелів, щоб наш слід було дуже важко відстежити [1]. VPN – namespace – це функція ядра Linux, що дозволяє ізолювати і віртуалізувати глобальні системи ресурси безлічі процесів. Приклади ресурсів які можна віртуалізувати: ID процесів, імена хостів, ID користувачів, доступ до мереж, межпроцесна взаємодія і файлові системи. Однією із загальних цілей простору імен є підтримка реалізації контейнерів - інструменту для віртуалізації на рівні операційної системизабезпечує групу процесів ілюзією того, що вони є єдиними процесами в системі[1].

Дослідження топології мереж є необхідністю для отримання розуміння чи є наше тунелі стабільними та конкурентноздатними. В ході дослідження мереж були взяті критерії за якими проводилось дослідження: Швидкість, завантаження, пінг, втрата пакетів та перевірка на анонімайзер. Були побудовані математичне очікування від кожної мережі, завдяки чому вдалося створити критерій якості за мережами.

Список літератури:

1. *Олександр Росляков. Віртуальні приватні мережі VPN, 2011, 328 стр.*
2. *Денис Колисниченко Анонімність і безпека в Інтернеті. 2014 р., 180стр.*