**ЛАБОРАТОРНА РОБОТА № 13**

**ТЕМА:** Захист ОС сервера засобами програмного файрволу.

**МЕТА:** Набути практичних навиків з налаштування захисту сервера засобами програмного файрволу iptables.

**ОБЛАДНАННЯ:** ПК конфігурації (Tyan Tiger i7525 (S2672ANR)/2 x Intel Xeon 2.8GHz, 1Gb – ОЗП (ECC)/4xHDD WD 320), ОС Ubuntu Linux 16.04 Server Edition.

**ХІД РОБОТИ:**

1. Встановлюю програмний файрвол на сервері під ОС Ubuntu.

2. Переглядаю список завантажених програм та порти, на яких вони слухають з’єднання.

3. Задаю правила на ПК з ОС Ubuntu Linux, що повинні фільтрувати всі пакети, які йдуть на 21, 22, 23 порти. Дозволити пакети, що йдуть на 80 та 445 порти.

iptables -A INPUT -p tcp --dport 21 -j DROP

iptables -A INPUT -p tcp --dport 22 -j DROP

iptables -A INPUT -p tcp --dport 23 -j DROP

iptables -A INPUT -p tcp --sport 80 -j ACCEPT

iptables -A INPUT -p tcp --sport 445 -j ACCEPT

4. Перевіряю програмою nmap з ПК адміністратора коректність заданих правил.

nmap –p 21,22,23 192.168.1.12

nmap –p 80,443 192.168.1.12

5. Вивожу статистику роботи файрвола iptables.

iptables –vnL –line-numbers

**ВИСНОВОК:** На цій лабораторній роботі я набув практичних навиків з налаштування захисту сервера засобами програмного файрволу iptables.