Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Факультет комп'ютерних наук

Кафедра безпеки інформаційних систем та технологій

Лабораторна робота № 3

з навчальної дисципліни

«Спеціалізовані мови програмування та проектування електронних елементів і систем»

Виконав:

Студент групи КБ-41

Кравченко Є.М.

Перевірив:

Професор

Олійников Р.В.

Харків – 2021 р.

**LABORATORY WORK #3**

**“PROTECTING LINUX SERVER FROM THE TCP SYN (SYN FLOOD) ATTACK”**

1. Preparing networking server in virtual computer (setting up IP and MAC addresses, checking http, ftp and telnet connections between Windows and Linux), like in the Lab #1.

2. Capture traffic of establishing normal TCP connection between the browser on your Windows workstation and the web server on Linux (using WireShark sniffer like in the Lab #1).

3. Learning information about hping2 utility for sending arbitrary IP packets from the command line in Linux (type *man hping2*).

4. Choosing neighbor brigade you will be working with. Organize TCP SYN attack on Linux server.

5. Checking the availability of the web server on their Linux via the browser on Windows computer (instead of http port you can choose telnet).

6. Using hping2 utility to send SYN packets to the port of the selected service on neighbor’s Linux.

7. Checking the availability of the attacked service. Usually, it will be available for the first attempt ☺ Checking, correctness of hping2 parameters one more time and begin sniffing (the next step).

8. Capture traffic of attack using Wireshark. Analyze them and find unnecessary IP packets which prevent your attack (try to find TCP RST packets).

9. Get rid of unnecessary IP packets in **two different** ways (with iptables and without it).

10. After successful organizing of attack on server by the neighbor’s brigade protecting server by switching on SYN cookies in Linux kernel. SYN cookies prevent such an attack by reserving memory for TCP connection on server only after receiving ACK packet (3rd step of handshake).

To switch on SYN cookies, type in the Linux command line:

*echo 1 > /proc/sys/net/ipv4/tcp\_syncookies*

Be attentive, Linux is case-sensitive, and don’t put unnecessary spaces.

11. Let neighbor’s brigade start attack again and check the availability of the server now. It **must be available**.