ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅՈՒՆ ԿՐԹՈՒԹՅԱՆ ԵՎ ԳԻՏՈՒԹՅԱՆ ՆԱԽԱՐԱՐՈՒԹՅՈՒՆ
ՀԱՅԱՍՏԱՆԻ ԱԶԳԱՅԻՆ ՊՈԼԻՏԵԽՆԻԿԱԿԱՆ ՀԱՄԱԼՍԱՐԱՆ
ՏՀՏԷ ԻՆՍՏԻՏՈՒՏ ՏԵՂԵԿԱՏՎՈՒԹՅԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԵՎ ԾՐԱԳՐԱՅԻՆ ԱՊԱՀՈՎՄԱՆ ԱՄԲԻՈՆ

Լաբորատոր աշխատանք 13

Ինստիտուտ՝ ՏՀՏԷ
Առարկա՝ Ծրագրային ապահովման անվտանգություն
Թեմա՝ Պարզ Firewall համակարգի մոդելավորում
Խումբ ՝ SS-355
Ուսանող՝ Մելքոնյան Սոնա

Երևան 2026

Ծրագիրը psutil գրադարանի միջոցով հավաքագրում է ակտիվ ցանցային կապերը, ցուցադրում է բաց պորտերը, որոշում է դրանց պրոտոկոլները և պահպանում արդյունքները JSON log ֆայլում:

```
sona@WIN-L4E9UMLMG68:/mnt/c/Users/user/Desktop/Software Security/lab13/dev/python/firewall1$ python3 firewal
l-1.py
Open ports:
{'port': 53, 'protocol': 'TCP/UDP', 'status': 'NONE'}
{'port': 53, 'protocol': 'TCP/UDP', 'status': 'LISTEN'}
{'port': 53, 'protocol': 'TCP/UDP', 'status': 'NONE'}
{'port': 40738, 'protocol': 'TCP/UDP', 'status': 'TIME_WAIT'}
{'port': 323, 'protocol': 'TCP/UDP', 'status': 'NONE'}
{'port': 53, 'protocol': 'TCP/UDP', 'status': 'LISTEN'}
{'port': 323, 'protocol': 'TCP/UDP', 'status': 'NONE'}
{'port': 53, 'protocol': 'TCP/UDP', 'status': 'LISTEN'}
{'port': 53, 'protocol': 'TCP/UDP', 'status': 'NONE'}
Monitoring traffic for 5 seconds...
Heavy ports: [(53, 30), (323, 10), (40738, 5)]
Saved to firewall_log_2026-05-17_20-03.json
```

dev > python > firewall1 > firewall_log_2026-05-17_20-03.json > open_ports > 5 > protocol


```
{
    "open_ports": [
        {
            "port": 53,
            "protocol": "TCP/UDP",
            "status": "NONE"
        },
        {
            "port": 53,
            "protocol": "TCP/UDP",
            "status": "LISTEN"
        },
        {
            "port": 53,
            "protocol": "TCP/UDP",
            "status": "NONE"
        },
        {
            "port": 40738,
            "protocol": "TCP/UDP",
            "status": "TIME_WAIT"
        },
        {
            "port": 323,
            "protocol": "TCP/UDP",
            "status": "NONE"
        },
        {
            "port": 53,
            "protocol": "TCP/UDP",
            "status": "LISTEN"
        },
        {
            "port": 323,
            "protocol": "TCP/UDP",
            "status": "NONE"
        },
        {
            "port": 53,
            "protocol": "TCP/UDP",
            "status": "LISTEN"
        },
        {
            "port": 53,
            "protocol": "TCP/UDP",
            "status": "NONE"
        }
    ],
    "heavy_ports": [
        [
            53,
            30
        ],
        [
            323,
            10
        ],
        [
            40738,
            5
        ]
    ],
    "rules": {
        "blocked_in": [
            80
        ],
        "blocked_out": [
            22
        ]
    }
```

iptables.cpp ծրագիրը ցույց է տալիս Linux firewall integration-ի օրինակ: iptables հրամանի միջոցով հնարավոր է արգելափակել TCP պորտերը:
Ծրագրում օգտագործվում են blocked_in և blocked_out կանոններ, որոնք նախատեսված են incoming և outgoing կապերի վերահսկման համար:

```
dev > cpp > linux > iptables.cpp > ...
// firewall_linux_real.cpp

// sudo iptables-save > /etc/iptables/rules.v4

#include <iostream>
#include <cstdlib>
#include <string>

using namespace std;

// ----------------------------
// Block IN
// ----------------------------
void block_port_in(int port) {
    string cmd = "sudo iptables -A INPUT -p tcp --dport " + to_string(port) + " -j DROP";
    system(cmd.c_str());
}

// ----------------------------
// Block OUT
// ----------------------------
void block_port_out(int port) {
    string cmd = "sudo iptables -A OUTPUT -p tcp --dport " + to_string(port) + " -j DROP";
    system(cmd.c_str());
}

// ----------------------------
// UNBLOCK
// ----------------------------
void unblock_port(int port) {
    string cmd1 = "sudo iptables -D INPUT -p tcp --dport " + to_string(port) + " -j DROP";
    string cmd2 = "sudo iptables -D OUTPUT -p tcp --dport " + to_string(port) + " -j DROP";

    system(cmd1.c_str());
    system(cmd2.c_str());
}

// ----------------------------
int main() {
    cout << "Blocking port 80 IN...\n";
    block_port_in(80);

    cout << "Blocking port 22 OUT...\n";
    block_port_out(22);

    cout << "Unblocking port 80...\n";
    unblock_port(80);

    return 0;
}
```

```
sonz@WIN-L4E9OMLMG68:/mnt/c/Users/user/Desktop/Software Security/lab13/dev/cpp/linux$ g++ iptables.cpp -o ip.cpp
sonz@WIN-L4E9OMLMG68:/mnt/c/Users/user/Desktop/Software Security/lab13/dev/cpp/linux$ ./ip.cpp
Blocking port 80 IN...
Blocking port 22 OUT...
Unblocking port 80...
iptables: Bad rule (does a matching rule exist in that chain?).
sonz@WIN-L4E9OMLMG68:/mnt/c/Users/user/Desktop/Software Security/lab13/dev/cpp/linux$
```

Firewall-ի տվյալները պահվում են timestamp-ով JSON ֆայլում, որը պարունակում է բաց պորտերը, ծանրաբեռնված պորտերը և firewall կանոնները:

Եզրակացություն

Լաբորատոր աշխատանքի ընթացքում իրականացվել է firewall համակարգի պարզ մոդելավորում Python և C++ լեզուներով: Ուսումնասիրվել են պորտերի աշխատանքը, TCP/UDP գաղափարը, firewall logic-ը և ցանցային տրաֆիկի վերլուծությունը: