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

Լաբորատոր աշխատանք 11

Ինստիտուտ՝ ՏՀՏԷ
Առարկա՝ Ծրագրային ապահովման անվտանգություն
Թեմա՝Reverse Engineering, Crackme և Simple Executable Packer
Խումբ ՝ SS-355
Ուսանող՝ Հովհաննիսյան Աննա

program.cpp program.cpp ֆայլը սովորական executable ծրագիր է, որը օգտագործվում է որպես packer-ի input: Այն տպում է "Original program is running!" հաղորդագրությունը: program.exe ֆայլն է կոդավորվում packer-ի միջոցով:

```
program.cpp > main()
#include <iostream>
using namespace std;

int main() {
    cout << "Original program is running!" << endl;
    return 0;
}
```

packer.cpp packer.cpp ֆայլը կատարում է simple executable packer-ի դեր: Այն բացում է program.exe ֆայլը binary ռեժիմով, կարդում է դրա ամբողջ բովանդակությունը, հետո յուրաքանչյուր byte-ի վրա կատարում է XOR գործողություն 0xAA key-ով: Արդյունքում ստացված կոդավորված տվյալները պահվում են packed.bin ֆայլում:

```
packer.cpp > main()
#include <iostream>
#include <fstream>
#include <vector>
using namespace std;

vector<char> read_file(const string& path) {
    ifstream file(path, ios::binary);
    return vector<char>((istreambuf_iterator<char>(file)),
                        istreambuf_iterator<char>());
}

void write_file(const string& path, const vector<char>& data) {
    ofstream file(path, ios::binary);
    file.write(data.data(), data.size());
}

void xor_encrypt(vector<char>& data, char key) {
    for (auto& b : data) {
        b ^= key;
    }
}

int main() {
    string input = "program.exe";
    string output = "packed.bin";
    char key = 0xAA;

    vector<char> data = read_file(input);
    xor_encrypt(data, key);
    write_file(output, data);

    cout << "Packed successfully!" << endl;
    return 0;
}
```

stub.cpp stub.cpp ֆայլը կատարում է unpacker կամ loader-իդեր: Այն բացում է packed.bin ֆայլը, նույն 0xAA key-ով կատարում է XOR decode, վերականգնում է սկզբնական executable-ը և պահում է այն որպես unpacked.exe: Դրանից հետո ծրագիրը աշխատեցնում է unpacked.exe ֆայլը:

```
stub.cpp > main()
#include <iostream>
#include <fstream>
#include <vector>
#include <cstdlib>
using namespace std;

void xor_decrypt(vector<char>& data, char key) {
    for (auto& b : data) {
        b ^= key;
    }
}

int main() {
    ifstream file("packed.bin", ios::binary);

    if (!file) {
        cout << "packed.bin not found!" << endl;
        return 1;
    }

    vector<char> data((istreambuf_iterator<char>(file)),
                      istreambuf_iterator<char>());

    xor_decrypt(data, 0xAA);

    ofstream out("unpacked.exe", ios::binary);
    out.write(data.data(), data.size());
    out.close();

    cout << "Unpacked successfully!" << endl;
    system("unpacked.exe");

    return 0;
}
```

password_helper.cpp password_helper.cpp ֆայլը օգտագործվում է crackme-ի password-ը reverse engineering մեթոդով վերականգնելու համար: Քանի որ crackme-ում password-ը ստուգվում է input[i] ^ 0x55 == key[i] բանաձևով, այստեղ կատարվում է հակառակ գործողությունը՝ key[i] ^ 0x55: Արդյունքում ստացվում է իրական password-ը՝ admin

```
password_helper.cpp > main()
#include <iostream>
using namespace std;

int main() {
    int key[] = {52, 49, 56, 60, 59};

    cout << "Recovered password: ";

    for (int i = 0; i < 5; i++) {
        char c = key[i] ^ 0x55;
        cout << c;
    }

    cout << endl;
    return 0;
}
```

crackme.cpp crackme.cpp ֆայլը պարզ crackme օրինակ է: Ծրագիրը օգտատիրոջից պահանջում է password և ստուգում է այն check() ֆունկցիայի միջոցով: Password-ը բաց տեսքով պահված չէ. այն ստուգվում է XOR մեթոդով: Եթե մուտքագրված password-ի յուրաքանչյուր սիմվոլը XOR արվի 0x55 key-ով և համընկնի key զանգվածի արժեքների հետ, ծրագիրը տպում է "Access Granted!", հակառակ դեպքում՝ "Access Denied!"

crackme.cpp > main()

```cpp
#include <iostream>
#include <string>
using namespace std;

bool check(string input) {
    int key[] = {52, 49, 56, 60, 59}; // password: admin

    if (input.length() != 5)
        return false;

    for (int i = 0; i < 5; i++) {
        if ((input[i] ^ 0x55) != key[i])
            return false;
    }

    return true;
}

int main() {
    string pass;

    cout << "Enter password: ";
    cin >> pass;

    if (check(pass)) {
        cout << "Access Granted!" << endl;
    } else {
        cout << "Access Denied!" << endl;
    }

    return 0;
}
```

```
sona@WIN-L4E9DMLMG68:/mnt/c/Users/user/Desktop/Software Security/lab12$ ./packer.exe
Packed successfully!
sona@WIN-L4E9DMLMG68:/mnt/c/Users/user/Desktop/Software Security/lab12$ ./stub.exe
Unpacked successfully!
sh: 1: unpacked.exe: not found
sona@WIN-L4E9DMLMG68:/mnt/c/Users/user/Desktop/Software Security/lab12$ ./crackme.exe
Enter password: admin
Access Granted!
sona@WIN-L4E9DMLMG68:/mnt/c/Users/user/Desktop/Software Security/lab12$ ./password_helper.exe
Recovered password: admin
```