
Botnet command & control szerver

Egy kiberbiztonsági cég gyakornokaként megkértek, hogy készíts egy szimulált **botnet command & control (C&C) szervert** C++ nyelven.

A szerver fertőzött gépeket (“zombi” PC-keket) tart nyilván, parancsokat küld nekik, és képes koordinált támadásokat (pl. DDoS) indítani.

Adatok

Az adatokat olvasd be a [zombies.txt](#) állományból. A fájl szerkezete a következő:

Minden sor egy új zombi gépet jelöl. A sorok szóközökkel vagy tabulátorral vannak elválasztva.

Formátum:

```
1 IP_cím ország CPU_százalék típus extra_adat
```

Például:

1	185.23.11.45	Romania	67	Windows	10
2	94.156.2.89	Ukraine	92	Linux	true
3	178.128.45.201	Russia	34	Windows	11
4	5.199.200.11	Hungary	88	Linux	false
5	212.77.1.33	Poland	55	Windows	10

A [típus](#) mező alapján kell eldönten, hogy Windows vagy Linux zombi objektum jön létre, és az [extra_adat](#) mező jelentése ehhez igazodik.

Alap- és származtatott osztályok

Hozz létre egy [Zombie](#) nevű **absztrakt** osztályt, amely minden zombi közös tulajdonságait és fügvényeit.

Származtass belőle **két** konkrét osztályt:

1. [WindowsZombie](#) Extra adattag: verzió (pl. “10”, “11”)
2. [LinuxZombie](#) Extra adattag: root jogunk van-e (true/false)

Kíráskor minden esetben írd ki az extra adatot is!

A szerver osztály

Készíts egy [C2Server](#) osztályt, amely a zombikat tárolja és irányítja. Kezdetben a gépek adatait a [zombies.txt](#) állományból olvassuk be. Lásd lentebb, miket tud a szerver csinálni.

Parancsszkript feldolgozása

A program egy második állományt is beolvas, `commands.txt` néven. Ez a fájl soronként olyan szöveges parancsokat tartalmaz, amelyeket a `C2Server` egymás után végrehajt. A parancsok minden egy szóból állnak, némelyiknek pedig van paramétere is.

Például:

```
1 PRINT_STATUS  
2 DDOS 1.2.3.4  
3 PRINT_OFFLINE  
4 DELETE_OFFLINE  
5 PRINT_STATUS
```

Támogatott parancsok:

- `PRINT_STATUS` – az összes zombi adatait kiírja
- `PRINT_ONLINE` - kiírja az online zombik adatait
- `PRINT_OFFLINE` - kiírja az offline zombik adatait
- `SET_CPU <IP> <CPU_PERCENTAGE>` – módosítja a CPU terhelést az adott IP című gépnek
 - ha nem létezik ilyen IP című gép, dobjon kivételt
- `GET_LINUX` – csak a Linux alapú zombikat listáját tériti vissza
- `GET_WINDOWS` – csak a Windows OS-es zombik listáját tériti vissza
- `DDOS <IP>` – szimulált támadást indít a megadott IP cím ellen csak az online zombik segítségével:
 - ha a CPU terheltség > 90% → túlterhelődött → offline, máskülönben online-nak számít
 - DDoS közben a gépek CPU terhelése felmegy 45%-kal. Vigyázzunk, hogy a CPU terhelése nem lehet 100% felé.
- `DELETE_OFFLINE` - törli az offline zombikat

Példa main.cpp teszteléshez

```
1 int main()  
2 {  
3     C2Server server;  
4  
5     // Parancsok feldolgozása  
6     server.processCommands("commands.txt");  
7  
8     return 0;  
9 }
```