**Keylogger folosind modul kernel**

**Descriere la modul general**

Keylogger sau „înregistrarea tastelor” este actul de înregistrare a tastelor apăsate pe tastatură, prin mijloace software sau hardware, de cele mai multe ori persoana monitorizată neștiind că apăsările lui/ei sunt înregistrate. Programul de înregistrare poate prelua ulterior datele înregistrate din zona sa de stocare.

Exista keyloggere bazate pe software sau pe hardware.

Cele bazate pe software sunt programe de calculator care funcționează cu software-ul computerului țintă.  Keylogger-urile hardware nu depind de niciun software instalat și există la nivelul hardware al computerului. Aceste keyloggere hardware pot fi adăugate fizic la tastatură sub forma unui circuit hardware sau.

**Keylogger folosind modul kernel**

Acesta este o categorie de keylogger care se ascunde în sistemul de operare prin obținerea accesului root. Programele care obțin acces root rezidă la nivel de kernel, nucleul fiind modulul central al sistemului de operare. Aceste keyloggere sunt greu de detectat și eliminat deoarece aplicațiile la nivel de utilizator nu au permisiuni pentru a modifica programele la nivel de kernel.

* **la nivelul Kernel** : Un program de pe mașină câștigă acces root (adică cu privilegii de administrator) și se ascunde în sistemul de operare, începând să intercepteze semnalele de apăsări de taste care trec prin kernel. Un keylogger care se află la nivelul nucleului este greu de detectat, în special pentru aplicațiile care nu au drepturi de administrator.

**Implementare si functionare**

Vom dezvolta programul software in limbajul C/C++. Va fi implementat ca un rootkit (**Rootkit-ul** este o colecție de software tipic rau intentionat conceput pentru a avea acces la un computer sau o parte a acestuia, care altfel nu ar fi posibil (de exemplu, de către un utilizator neautorizat să se autentifice).) care sabotează nucleul sistemului de operare pentru a obține acces la hardware-ul computerului neautorizat. Prin urmare, devine foarte puternic, putând acționa ca un driver de tastatură și obținând acces la orice informație tastată care este trimisă sistemului de operare.

**Instalare**

Va fi instalat pe un sistem de operare Linux.