KEYLOGGER

-proiect proiectarea sistemelor de operare-

Echipa: Bureaca Angela Emilia

Ionel Ana-Maria

Grupa: C113-C

Îndrumator: Vaman Adina

CUPRINS

Capitolul 1 – Introducere
1.1. Scopul proiectului
1.1. Structura documentului

Capitolul 2 - Descrierea generală a produsului software
2.1. Introucere
2.2. Descrierea produsului software
2.2. Detaliera platformei HW/SW

Capitolul 3. Resurse necesare dezvoltării proiectului

Capitolul 4 - Detalierea cerințelor specifice

Capitolul 1 - Introducere

1.1 Scopul proiectului

Un keylogger este un program de calculator conceput pentru a monitoriza intrările de la tastatură, în general într-un mod ascuns pentru a se asigura că persoana monitorizată nu este conștientă de activitate Aceste programe monitorizează evenimentele de nivel inferior de la tastatură și poate rula oriunde, de la spațiul kernel la spațiul utilizator, în funcție de design.

Astfel de programe sunt utilizate în general în exercițiile de audit de securitate. Aceștia folosesc diverse instrumente de atac pentru a compromite sistemul țintă, pentru a se infiltra în infrastructură și pentru a captura date prețioase pentru a găsi și a expune diferitele lacune în monitorizarea securității întregii organizații țintă. Keylogger-urile sunt folosite pentru a înregistra acreditările contului, acreditările de rețea etc. care sunt apoi folosite pentru infiltrarea ulterioară a infrastructurii.

1.2 Structura documentului

Documentul este structurat pe trei capitole: capitolul 1 prezintă elemente introductive precum scopul proiectului, capitolul 2 prezintă o descriere detaliată a aplicației, capitolul 3 prezinta resursele necesare dezvoltarii proiectului, iar capitolul 4 prezintă cerințele exacte ale aplicației

Capitolul 2 – Descrierea generală a produsului software

2.1. Introducere

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.

2.2 Detalierea platformei HW/SW

Aplicația este dezvoltată pentru dispozitivele pe care care rulează sistemul de operare Linux. În ceea ce privește componenta hardware, Aplicatia va fi dezvoltata pe o masina virtuala de Ubuntu, folosind VMWare, este nevoie de un procesor cu o frecvență de 1.5 GHz sau mai mare, și o memorie RAM de peste 4 GB.

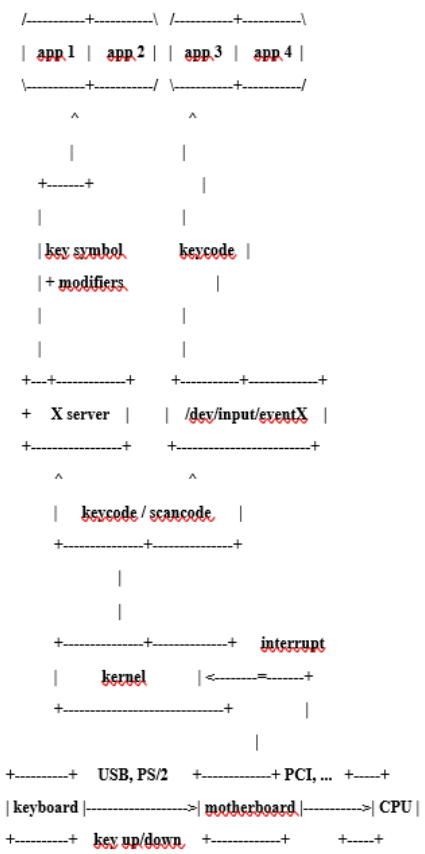
Vom dezvolta programul software in limbajul C/C++. Va fi implementat ca un rootkit (**Rootkit-ul** este o colecție de software tipic rau intentionat conceput pentru a avea acces la un computer sau o parte a acestuia, care altfel nu ar fi posibil (de exemplu, de către un utilizator neautorizat să se autentifice) 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.

2.3 Descrierea produsului

Keylogger-ul folosind modul kernel 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.

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.

O prezentare generală de bază a modului în care o tastatură se potrivește în schema mai mare este prezentată mai jos:



Tastatura nu trece codul ASCII al tastei apăsate, ea transmite un octet unic pentru fiecare eveniment numit cod-cheie. Când se execută un eveniment asupra unei taste, codul se transmite plăcii de baza. Placa de baza va genera o intrerupere la CPU. CPU lansează manevratorul de întreruperi (provine din nucleu însuși și este înregistrat prin popularea tabelului de descriptori de întreruperi). Acesta preia informațiile transmise de tastatura și le transmite nucleului care le expune printr-o cale specială. (/dev/input/eventX).

Un keylogger se poate scrie în două moduri:

1. Găsind care fișier /dev/input/eventX este un dispozitiv cu tastatură și citind direct din acel fișier
2. Cerând serverului X însuși să ne transmită date despre evenimente

Implementarea keylogger-ului nostru va fi bazata pe fisierul /dev/input/eventX.

Capitolul 3. Resurse necesare dezvoltarii proiectului

În vederea realizării aplicației avem nevoie de următoarele medii de lucru/resurse:

- VMWare Workstation 16 Player
- O versiune de kernel “proprie” - vom implementa propriul modul de kernel.

Capitolul 4 - Detalierea cerințelor specifice

Deoarece în Linux totul este un fișier, și apăsările de taste sunt un fișier în sine. Acestea sunt stocate în /dev/input alături de toate dispozitivele de intrare. Informațiile legate de maparea tastaturii se găsesc in fișierul /proc/bus/input/devices, maparea se realizează între numele tastei și evenimentul produs la nivelul sistemului.

În implementarea keylogger-ului nostru avem în vedere urmatoarele aspecte:

- Datele (apasările de taste) vor fi stocate intr-un fisier jurnal numit “Keylogger.txt” in folderul /PSOP
- Cream o structura în care citim fișierul /dev/input/event, unde event este evenimentul de pe tastaura mea, și adauga tastele la fisierul jurnal din /tmp
- Evenimentele au 2 campuri, ev.type si ev.value. În ev.type reținem mișcarea luată de pe tastatură in EV_KEY, ev.value este setată implicit pe 0 deoarece dupa fiecare apăsare, exista și o eliberare a tastei, pentru a preveni inregistrarea de mai multe ori a aceleași valori.
- Apasarile de taste sunt mapate ca numere naturale corespunzatoare fiecarei taste. Aceasta mapare se regăsește în fișierul /usr/include/linux.
- Pentru a ne ușura implementarea, realizăm o harta a tastelor în codul nostru corespunzătoare valorii cheii numerice.
- Maparea va fi actualizată ulterior pentru a reține și alte evenimente realizate din tastatura (spatiu, \n ...)
- Vom construi diferite tamplate-uri, în funcție de tastele introduse, iar stocarea lor va fi redirectata spre fișiere specifice în funcție de tamplate (de exemplu, dacă un untilizator introduce o adresă de mail, aceasta va fi stocată în jurnalul destinat, keylogger-ul va recunoaște adresa de mail ca fiind o combinație de cifre și litere urmată de @ combinație litere . 2/3 litere).