

Laborator I: Introdúcere

Iosif George-Andrei

Tabelă de Conținut

Tabelă de Conținut

1. BinExpLabs 101

Tabelă de Conținut

1. BinExpLabs 101
2. Noțiuni Introductive

Tabelă de Conținut

1. BinExpLabs 101
2. Noțiuni Introductive
3. Exploatarea Executabilelor

Tabelă de Conținut

1. BinExpLabs 101
2. Noțiuni Introductive
3. Exploatarea Executabilelor
4. Instrumente

BinExpLabs 101

1. Laboratoare (50% din notă)

1. Laboratoare (50% din notă)
 - ▣ Rezolvarea în timpul laboratorului

1. Laboratoare (50% din notă)

- ❖ Rezolvarea în timpul laboratorului
- ❖ Participarea la *quiz*-uri

1. Laboratoare (50% din notă)
 - ❖ Rezolvarea în timpul laboratorului
 - ❖ Participarea la *quiz*-uri
2. Temă de casă (50% din notă)

1. Laboratoare (50% din notă)
 - ❖ Rezolvarea în timpul laboratorului
 - ❖ Participarea la *quiz*-uri
2. Temă de casă (50% din notă)
 - ❖ Detalierea rezolvării

1. Laboratoare (50% din notă)
 - ❖ Rezolvarea în timpul laboratorului
 - ❖ Participarea la *quiz*-uri
2. Temă de casă (50% din notă)
 - ❖ Detalierea rezolvării
 - ❖ Fără plagiat

Regulile Jocului

- ▣ Atenție în cadrul laboratoarelor

Regulile Jocului

- Atenție în cadrul laboratoarelor
- Respect reciproc

Must-have

 Resurse

❏ Resurse

- ❏ Mașină virtuală cu Linux

❖ Resurse

- ❖ Mașină virtuală cu Linux
- ❖ Python 3 cu librăria pwntools

❖ Resurse

- ❖ Mașină virtuală cu Linux
- ❖ Python 3 cu librăria pwntools
- ❖ Ghidra

❖ Resurse

- ❖ Mașină virtuală cu Linux
- ❖ Python 3 cu librăria pwntools
- ❖ Ghidra
- ❖ PEDA

Nice to Have

- ❖ Cunoștințe de limbaj de asamblare

- ❏ Cunoștințe de limbaj de asamblare
- ❏ Cunoștințe despre sisteme de operare

- ❖ Cunoștințe de limbaj de asamblare
- ❖ Cunoștințe despre sisteme de operare
- ❖ Experiență cu Linux

- ❖ Cunoștințe de limbaj de asamblare
- ❖ Cunoștințe despre sisteme de operare
- ❖ Experiență cu Linux
- ❖ Experiență cu Python 3

Noțiuni Introductive

Procese. Executable

Procese. Executabile

- ❖ *Proces*: Set de instrucțiuni ce sunt grupate pentru a fi executate pe procesor, în cadrul sistemului de operare gazdă, cu scopul de a transforma date de intrare în date de ieșire.

Procese. Executabile

- ❖ *Proces*: Set de instrucțiuni ce sunt grupate pentru a fi executate pe procesor, în cadrul sistemului de operare gazdă, cu scopul de a transforma date de intrare în date de ieșire.
- ❖ *Executabil*: Fișier care încapsulează instrucțiuni ce trebuiesc executate de procesor și pe baza căruia este creat un proces. Numit și binar.

Procese. Executabile

- ❖ *Proces*: Set de instrucțiuni ce sunt grupate pentru a fi executate pe procesor, în cadrul sistemului de operare gazdă, cu scopul de a transforma date de intrare în date de ieșire.
- ❖ *Executabil*: Fișier care încapsulează instrucțiuni ce trebuiesc executate de procesor și pe baza căruia este creat un proces. Numit și binar.
- ❖ Cele mai comune formate

Procese. Executabile

- ❖ *Proces*: Set de instrucțiuni ce sunt grupate pentru a fi executate pe procesor, în cadrul sistemului de operare gazdă, cu scopul de a transforma date de intrare în date de ieșire.
- ❖ *Executabil*: Fișier care încapsulează instrucțiuni ce trebuiesc executate de procesor și pe baza căruia este creat un proces. Numit și binar.
- ❖ Cele mai comune formate
 - ❖ Portable Executable (abreviat PE, specific Windows)

Procese. Executabile

- ❖ *Proces*: Set de instrucțiuni ce sunt grupate pentru a fi executate pe procesor, în cadrul sistemului de operare gazdă, cu scopul de a transforma date de intrare în date de ieșire.
- ❖ *Executabil*: Fișier care încapsulează instrucțiuni ce trebuiesc executate de procesor și pe baza căruia este creat un proces. Numit și binar.
- ❖ Cele mai comune formate
 - ❖ Portable Executable (abreviat PE, specific Windows)
 - ❖ Executable and Linkable Format (abreviat ELF, specific Unix)

Formatul ELF

```
sketch();
```

Memoria unui Proces

```
sketch();
```

Stiva unui Proces


```
sketch();
```

Exploatarea Executabilelor

Terminologie

- ❖ *Vulnerabilitate*: Slăbiciune a unui sistem informatic, ce poate provoca o funcționare incorectă a lui.

- ❖ *Vulnerabilitate*: Slăbiciune a unui sistem informatic, ce poate provoca o funcționare incorectă a lui.
- ❖ *Exploatare*: Atacarea cu succes a unui sistem informatic, prin intermediul unei vulnerabilități.

- ❖ *Vulnerabilitate*: Slăbiciune a unui sistem informatic, ce poate provoca o funcționare incorectă a lui.
- ❖ *Exploatare*: Atacarea cu succes a unui sistem informatic, prin intermediul unei vulnerabilități.
- ❖ *Exploatarea Executabilelor*: Provocarea de către un atacator a execuției incorecte a unui executabil.

Suprafața de Atac

- ❖ Set de puncte (numite vectori de atac) de la marginea unui sistem informatic pe care un atacator le poate folosi pentru a interacționa cu el (obținerea accesului, extragerea datelor, perturbarea funcționării).

Suprafața de Atac

- ❖ Set de puncte (numite vectori de atac) de la marginea unui sistem informatic pe care un atacator le poate folosi pentru a interacționa cu el (obținerea accesului, extragerea datelor, perturbarea funcționării).
- ❖ Vectori uzuali de atac

Suprafața de Atac

- ❖ Set de puncte (numite vectori de atac) de la marginea unui sistem informatic pe care un atacator le poate folosi pentru a interacționa cu el (obținerea accesului, extragerea datelor, perturbarea funcționării).
- ❖ Vectori uzuali de atac
 - ❖ stdin

- ❖ Set de puncte (numite vectori de atac) de la marginea unui sistem informatic pe care un atacator le poate folosi pentru a interacționa cu el (obținerea accesului, extragerea datelor, perturbarea funcționării).
- ❖ Vectori uzuali de atac
 - ❖ stdin
 - ❖ Argumente

- ❖ Set de puncte (numite vectori de atac) de la marginea unui sistem informatic pe care un atacator le poate folosi pentru a interacționa cu el (obținerea accesului, extragerea datelor, perturbarea funcționării).
- ❖ Vectori uzuali de atac
 - ❖ stdin
 - ❖ Argumente
 - ❖ Variabile de mediu

- ❖ Set de puncte (numite vectori de atac) de la marginea unui sistem informatic pe care un atacator le poate folosi pentru a interacționa cu el (obținerea accesului, extragerea datelor, perturbarea funcționării).
- ❖ Vectori uzuali de atac
 - ❖ stdin
 - ❖ Argumente
 - ❖ Variabile de mediu
 - ❖ Fișiere (de configurație, baze de date)

- ❖ Set de puncte (numite vectori de atac) de la marginea unui sistem informatic pe care un atacator le poate folosi pentru a interacționa cu el (obținerea accesului, extragerea datelor, perturbarea funcționării).
- ❖ Vectori uzuali de atac
 - ❖ stdin
 - ❖ Argumente
 - ❖ Variabile de mediu
 - ❖ Fișiere (de configurație, baze de date)
 - ❖ Întreruperi

- ❖ Set de puncte (numite vectori de atac) de la marginea unui sistem informatic pe care un atacator le poate folosi pentru a interacționa cu el (obținerea accesului, extragerea datelor, perturbarea funcționării).
- ❖ Vectori uzuali de atac
 - ❖ stdin
 - ❖ Argumente
 - ❖ Variabile de mediu
 - ❖ Fișiere (de configurație, baze de date)
 - ❖ Întreruperi
 - ❖ Dispozitive

Motivație

- Înțelegerea mentalității de atacator

- Înțelegerea mentalității de atacator
- *Bug bounty*

- ❖ Înțelegerea mentalității de atacator
- ❖ *Bug bounty*
 - ❖ CVE-2019-5790, ca *integer overflow* în Google Chrome, ce permitea execuția de cod de la distanță

- ❖ Înțelegerea mentalității de atacator
- ❖ *Bug bounty*
 - ❖ CVE-2019-5790, ca *integer overflow* în Google Chrome, ce permitea execuția de cod de la distanță
- ❖ *Zero days*

- ❖ Înțelegerea mentalității de atacator
- ❖ *Bug bounty*
 - ❖ CVE-2019-5790, ca *integer overflow* în Google Chrome, ce permitea execuția de cod de la distanță
- ❖ *Zero days*
 - ❖ *Marketplaces*, precum Zerodium

- ❖ Înțelegerea mentalității de atacator
- ❖ *Bug bounty*
 - ❖ CVE-2019-5790, ca *integer overflow* în Google Chrome, ce permitea execuția de cod de la distanță
- ❖ *Zero days*
 - ❖ *Marketplaces*, precum Zerodium
 - ❖ Utilizarea în atacuri avansate, precum Stuxnet

Instrumente

- ▣ `strings`: Extragerea șirurilor de caractere printabile din fișiere.

- ❖ `strings`: Extragerea șirurilor de caractere printabile din fișiere.
- ❖ `nm`: Extragerea simbolurilor din fișierele obiect (atât executabile, cât și librării).

- ❖ `strings`: Extragerea șirurilor de caractere printabile din fișiere.
- ❖ `nm`: Extragerea simbolurilor din fișierele obiect (atât executabile, cât și librării).
- ❖ `ldd`: Extragerea dependențelor către librării dinamice.

- ❖ `strings`: Extragerea șirurilor de caractere printabile din fișiere.
- ❖ `nm`: Extragerea simbolurilor din fișierele obiect (atât executabile, cât și librării).
- ❖ `ldd`: Extragerea dependențelor către librării dinamice.
- ❖ `objdump`: Extrage informații din fișiere obiect. Poate fi folosit pentru dezasamblare.

- ❖ `strings`: Extragerea șirurilor de caractere printabile din fișiere.
- ❖ `nm`: Extragerea simbolurilor din fișierele obiect (atât executabile, cât și librării).
- ❖ `ldd`: Extragerea dependențelor către librării dinamice.
- ❖ `objdump`: Extrage informații din fișiere obiect. Poate fi folosit pentru dezasamblare.
- ❖ `Ghidra`: Instrument pentru inginerie inversă, cu funcționalități de dezasamblare și decompilare.

- ↳ trace: Interceptarea apelurilor către librării dinamice.

- ❖ `ltrace`: Interceptarea apelurilor către librării dinamice.
- ❖ `strace`: Interceptarea apelurilor de sistem.

- ❖ `ltrace`: Interceptarea apelurilor către librării dinamice.
- ❖ `strace`: Interceptarea apelurilor de sistem.
- ❖ `netstat`: Oferă detalii despre rețelistică, util pentru urmărirea conexiunilor efectuate.

- ❖ `ltrace`: Interceptarea apelurilor către librării dinamice.
- ❖ `strace`: Interceptarea apelurilor de sistem.
- ❖ `netstat`: Oferă detalii despre rețelistică, util pentru urmărirea conexiunilor efectuate.
- ❖ `gdb`: Depanează programe, putând fi folosit împreună cu PEDA.

- ❖ `pwntools`: Librărie Python3 ce ușurează exploatarea programelor

- ❖ `pwntools`: Librărie Python3 ce ușurează exploatarea programelor
- ❖ `man`: Interfață pentru manualele comenzilor.

Exerciții

1. Număr de Șiruri de Caractere Printabile
2. Tipuri de Șiruri de Caractere Printabile
3. Număr de Simboluri
4. Proveniența Simbolurilor
5. Automatizarea Analizei Dinamice cu pwntools
6. Librării Dinamice
7. Dezasamblarea Programelor
8. Apeluri de Sistem
9. Conexiuni

- ❖ Folosiți comanda `man` pentru a primi ajutor la rularea anumitor comenzi.

- ❖ Folosiți comanda `man` pentru a primi ajutor la rularea anumitor comenzi.
- ❖ Folosiți documentația `pwntools` pentru a identifica metodele de care aveți nevoie.

Recapitulare

Recapitulare

Recapitulare

