

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

Notare

Notare

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

Notare

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

Regulile Jocului

- ▣ Atenție în cadrul laboratoarelor

Regulile Jocului

- Atenție în cadrul laboratoarelor
- Respect reciproc

Must-have

Must-have

 Resurse

Must-have

❏ Resurse

- ❏ Mașină virtuală cu Linux

Must-have

❖ Resurse

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

Must-have

❖ 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

Nice to Have

- ❖ Cunoștințe de limbaj de asamblare

Nice to Have

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

Nice to Have

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

Nice to Have

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

Noțiuni Introductive

Procese. Executabile

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

Formatul ELF

```
sketch();
```

Memoria unui Proces

Memoria unui Proces

```
sketch();
```

Stiva unui Proces

Stiva unui Proces

```
sketch();
```

Exploatarea Executabilelor

Terminologie

Terminologie

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

Terminologie

- ❖ **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.

Terminologie

- ❖ **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

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

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
 - ❖ Argumente

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
 - ❖ Argumente
 - ❖ Variabile de mediu

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
 - ❖ Argumente
 - ❖ Variabile de mediu
 - ❖ Fișiere (de configurație, baze de date)

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
 - ❖ Argumente
 - ❖ Variabile de mediu
 - ❖ Fișiere (de configurație, baze de date)
 - ❖ Întreruperi

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
 - ❖ Argumente
 - ❖ Variabile de mediu
 - ❖ Fișiere (de configurație, baze de date)
 - ❖ Întreruperi
 - ❖ Dispozitive

Motivație

Motivație

- Înțelegerea **mentalității de atacator**

Motivație

- ❖ Înțelegerea **mentalității de atacator**
- ❖ ***Bug bounty***

Motivație

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

Motivație

- ❖ 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**

Motivație

- ❖ 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

Motivație

- ❖ 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

Pur Statice

- ▣ **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.

Pur Dinamice

❖ **ltrace**: Interceptarea apelurilor către librării dinamice.

Pur Dinamice

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

Pur Dinamice

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

Pur Dinamice

- ❖ **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

Recomandări

Recomandări

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

Recomandări

- ❖ 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

