Session 14
Windows Exploitation

Security Summer School
7th of August 2014

ACS/Ixia/Hexcellents

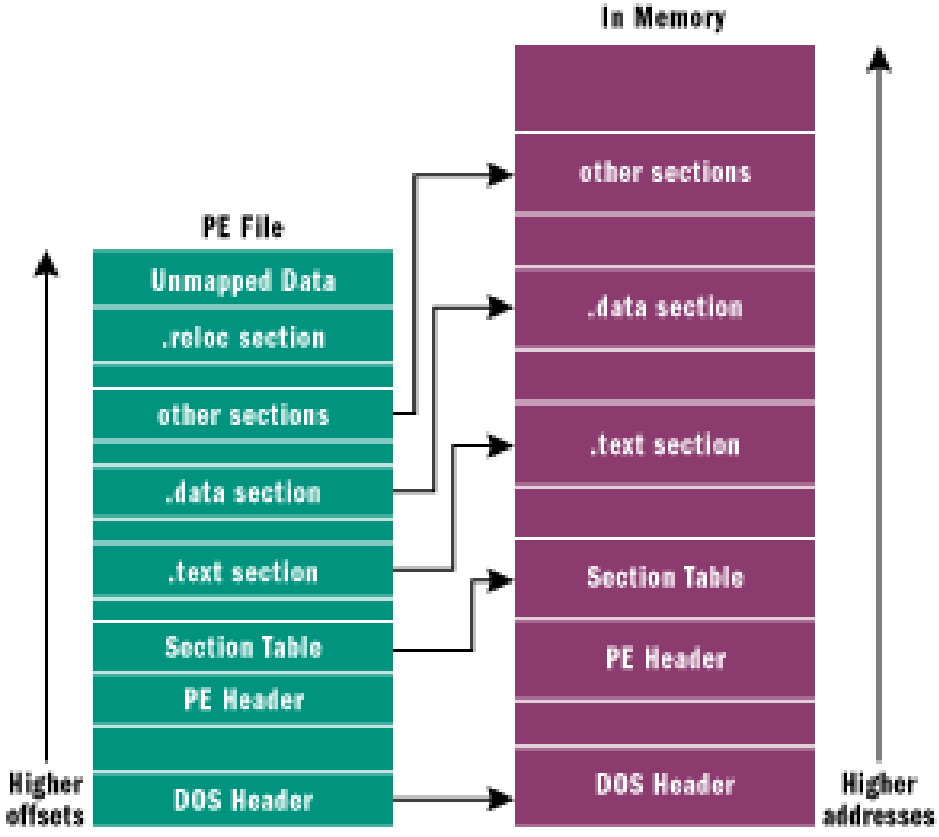
Outline

- PE History
- PE Mapping
- PE Headers
- IAT
- EAT
- PEB/TEB
- Windows Shellcode
- SEH Overflow

PE Basics - History

- Derived from the COFF format
- Is consistent across hardware architectures
- Has two basic forms
    - PE32
    - PE32+

PE Mapping


In Memory
other sections
.data section
.text section
Section Table
PE Header
DOS Header
Higher addresses
PE File
Unmapped Data
.reloc section
other sections
.data section
.text section
Section Table
PE Header
DOS Header
Higher offsets

PE Headers

- **Image DOS Header**
  - **e_lfanew** - offset to next header

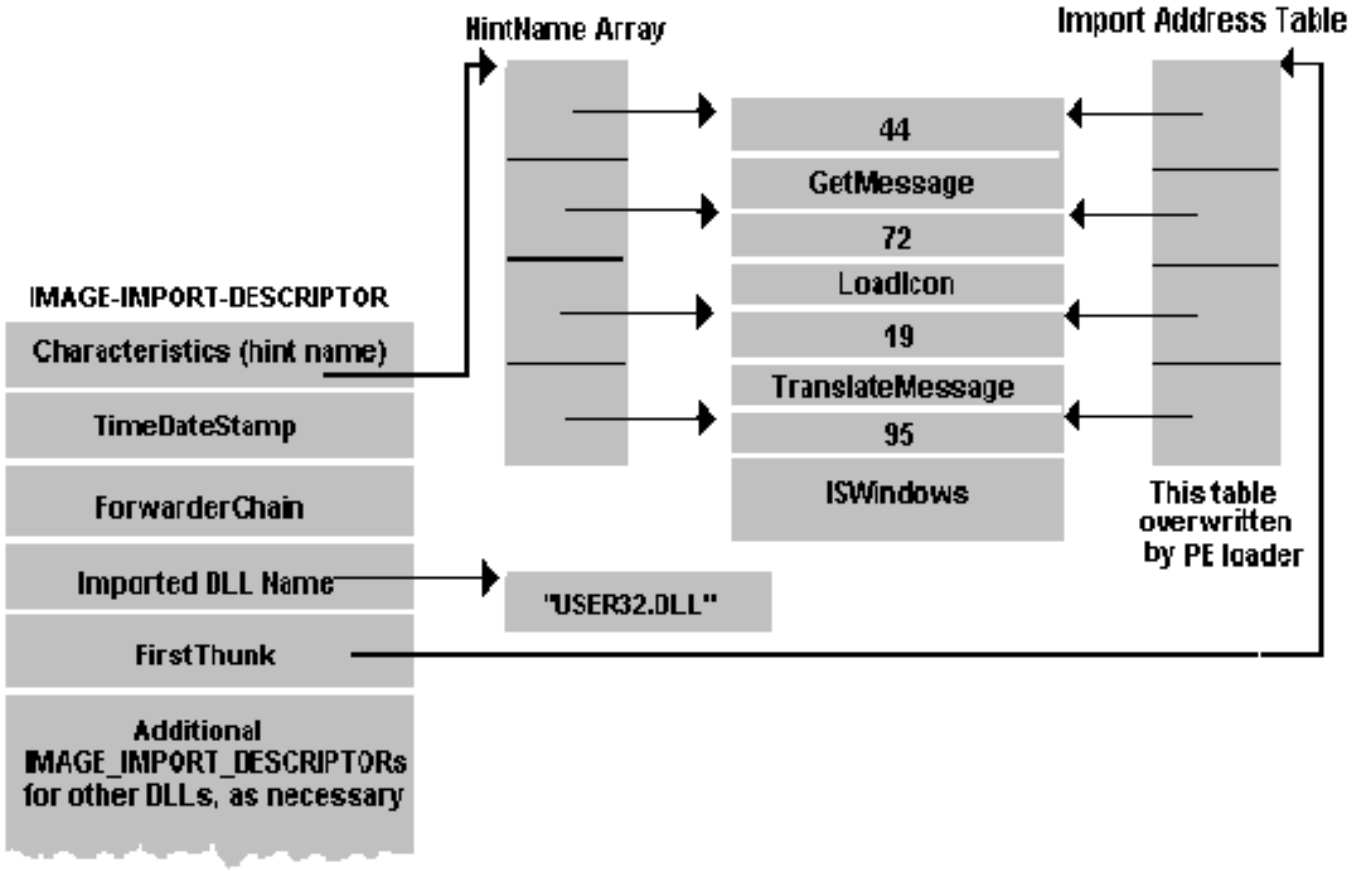
- **Image NT Header**
  - **Signature**
  - **FileHeader -** RVA
  - **OptionalHeader** RVA

- **Image File Header**
  - **Machine**
  - **TimeDateStamp**
  - **NumberOfSections**
  - **Characteristics**

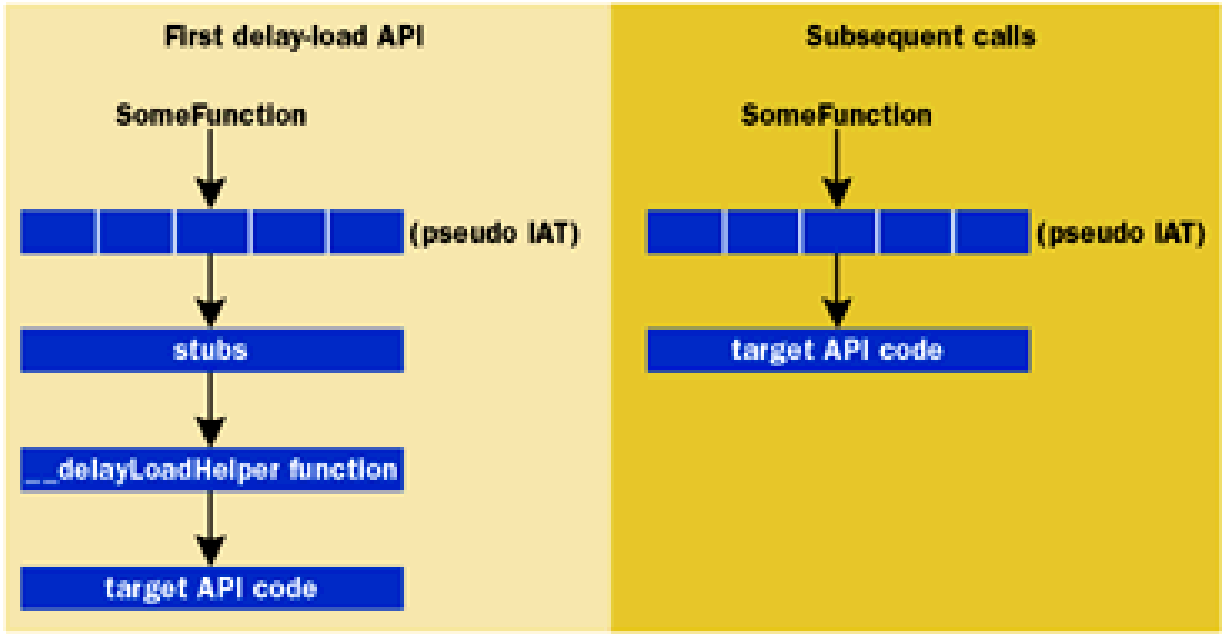
PE Headers

- **Image Optional Header**
  - **Magic**
  - **AddressOfEntryPoint – RVA**
  - **SizeOfImage**
  - **SectionAlignment**
  - **FileAlignment**
  - **ImageBase**
  - **DLLCharacteristics**

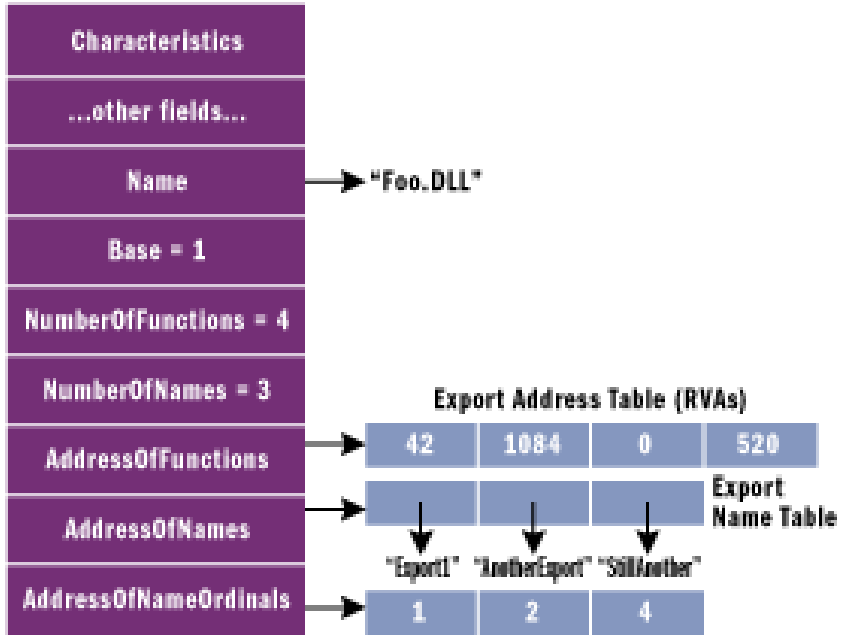
IAT (import address table)



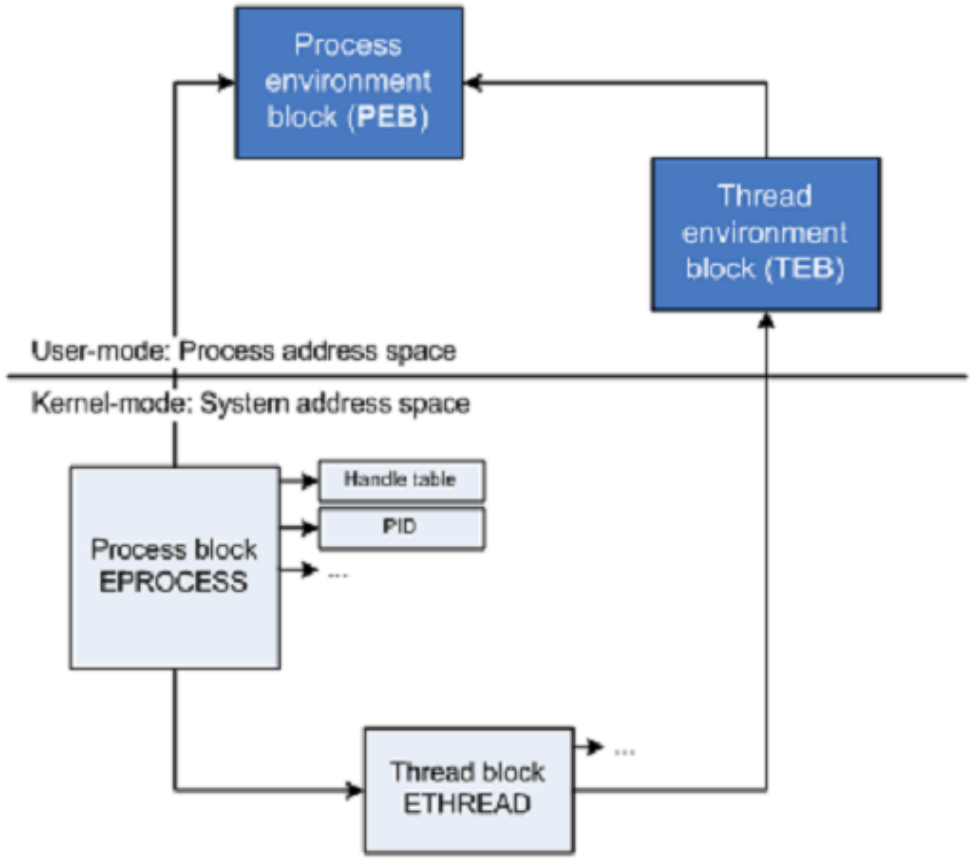
IAT (import address table)



EAT (Export address table)



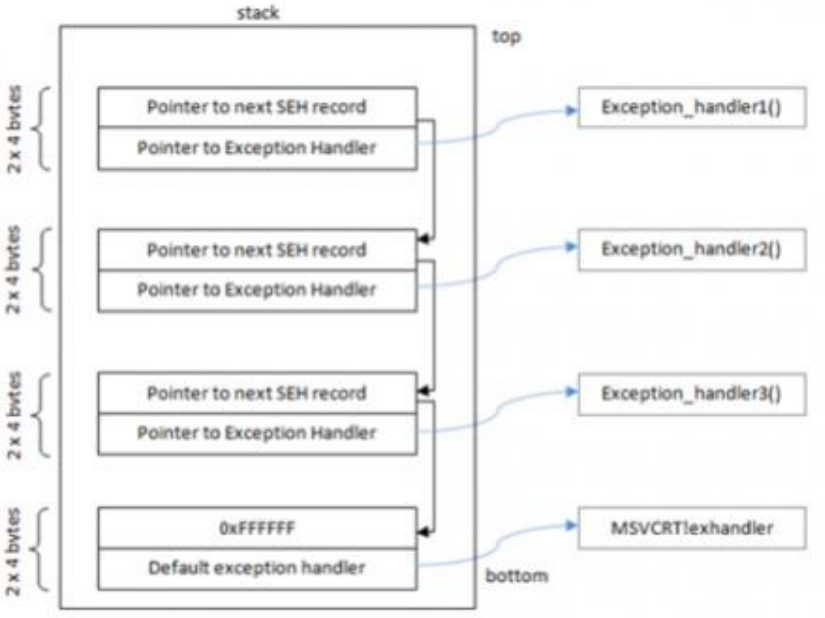
PEB/TEB

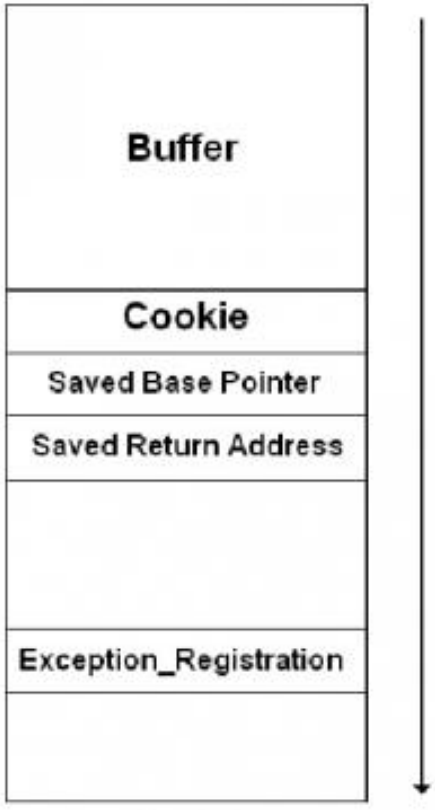

Process environment block (PEB)
Thread environment block (TEB)
User-mode: Process address space
Kernel-mode: System address space
Handle table
PID
...
Process block EPROCESS
Thread block ETHREAD
...

Windows Shellcode

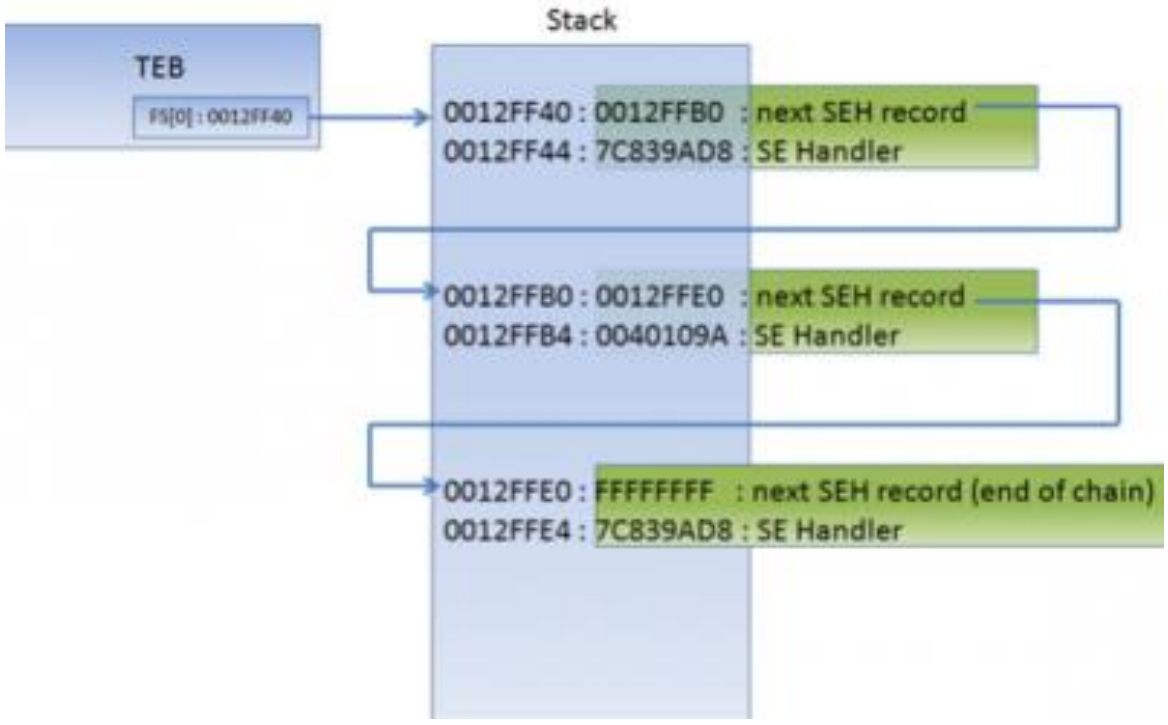
```
0000000: 31 c0 31 db 31 c9 31 d2 b0 04 b3 01 68 64 21 21
0000010: 21 68 4f 77 6e 65 89 e1 b2 08 cd 80 b0 01 31 db
0000020: cd 80
```

SEH Overflow





SEH Overflow



SEH Overflow