

(S\$\$)

ixia



Hexcellents

Session 14

Windows
Exploitation

Security Summer
School
7th of August 2014
ACS/Ixia/Hexcellents

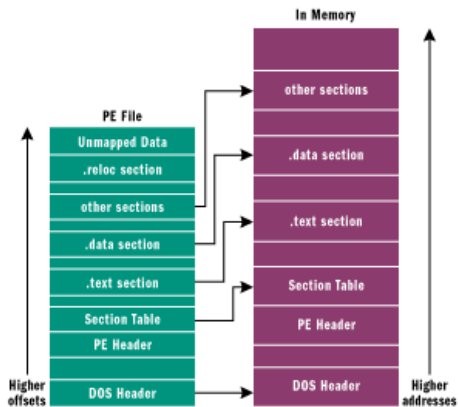
Outline

- 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



PE Headers

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

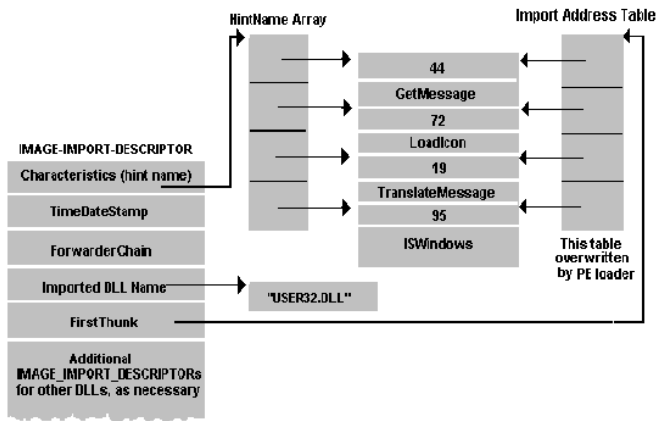
- **Image NT Header**
 - **Signature**
 - **FileHeader** - RVA
 - **OptionalHeader** RVA

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

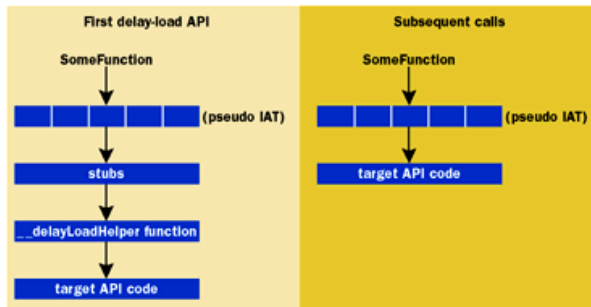
PE Headers

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

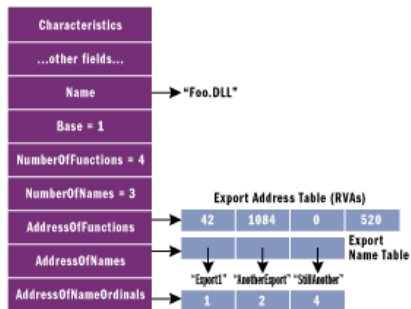
IAT (import address table)



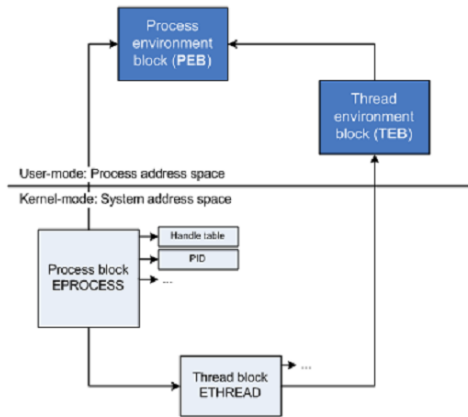
IAT (import address table)



EAT (Export address table)



PEB/TEB

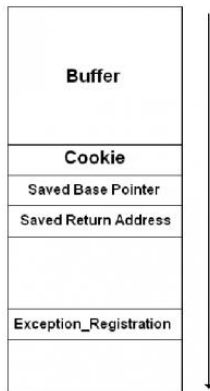
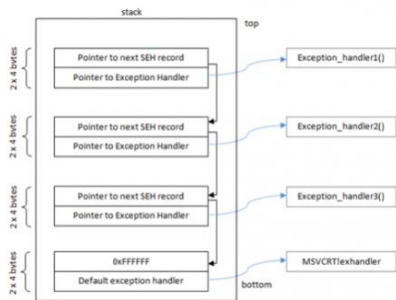


Windows Shellcode

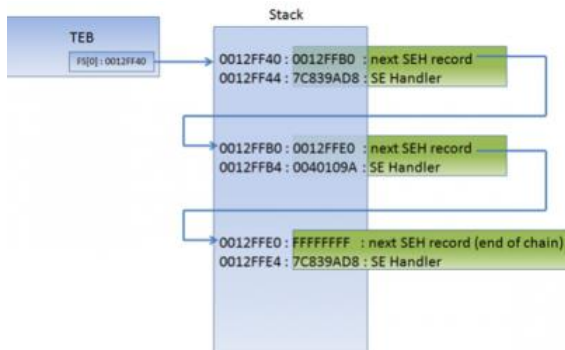
```
00000000: 31 c0 31 db 31 c9 31 d2 b0 04 b3 01 68 64 21 21
00000010: 21 68 4f 77 6e 65 89 e1 b2 08 cd 80 b0 01 31 db
00000020: cd 80
```

```
33 c0 64 8b 1d 30 00 00 89 5d dc 8b 4b 0c 89
4d c4 8b 51 1c 89 55 f4 8b 32 89 75 f0 8b 46 08
89 45 b0 8b 58 3c 89 5d c8 8b 4c 18 78 03 c8 89
4d a4 8b 71 1c 03 f0 89 75 f8 8b 51 20 03 d0 89
55 b8 8b 79 24 03 f8 89 7d e0 8b 59 14 89 5d ac
c7 45 e4 00 00 00 eb 09 8b 45 e4 83 c0 01 89
45 e4 8b 4d e4 3b 4d ac 0f 83 c8 00 00 00 8b 55
e4 8b 45 b8 8b 0c 90 89 4d d4 8b 55 b0 03 55 d4
89 55 98 68 48 c0 40 00 8b 45 98 50 e8 6a 02 00
00 83 c4 08 85 c0 75 42 8b 4d 98 51 8b 55 e4 52
68 58 c0 40 00 e8 84 01 00 00 83 c4 0c 8b 45 e4
8b 4d e0 0f b7 14 41 8b 45 f8 8b 0c 90 89 4d bc
8b 55 bc 03 55 b0 89 55 bc 8b 45 bc 50 68 68 c0
40 00 e8 57 01 00 00 83 c4 08 68 88 c0 40 00 8b
4d 98 51 e8 13 02 00 00 83 c4 08 85 c0 75 42 8b
55 98 52 8b 45 e4 50 68 98 c0 40 00 e8 2d 01 00
00 83 c4 0c 8b 4d e4 8b 55 e0 0f b7 04 4a 8b 4d
f8 8b 14 81 89 55 cc 8b 45 cc 03 45 b0 89 45 cc
8b 4d cc 51 68 a8 c0 40 00 e8 00 01 00 00 83 c4
08 e9 23 ff ff ff 8b 45 cc 8b 5d e8 53 ff d0 89
45 d4 8b 55 d4 52 68 c8 c0 40 00 e8 de 00 00 00
83 c4 08 8b 45 d4 8b 5d 9c 53 50 8b 45 bc ff d0
89 45 d4 8b 45 d4 50 68 f0 c0 40 00 e8 bd 00 00
00 83 c4 08 8b 45 d4 33 db 8b 4d fc 8b 55 ec 53
52 51 53 ff d0
```

SEH Overflow



SEH Overflow



SEH Overflow

