

Stručný obsah

Kapitola 01	Nastavení vývojového prostředí	15
Kapitola 02	Debuggery a jejich design	27
Kapitola 03	Tvorba vlastního debuggeru na Windows	39
Kapitola 04	PYDBG: debugger v Pythonu na Windows	73
Kapitola 05	Immunity Debugger: to nejlepší z obou světů	87
Kapitola 06	Hákování	103
Kapitola 07	Injektáž DLL a kódu	115
Kapitola 08	Fuzzing	131
Kapitola 09	Framework Sulley	145
Kapitola 10	Fuzzing ovladačů Windows	159
Kapitola 11	IDAPython: skriptování IDA Pro	175
Kapitola 12	PyEmu: skriptovatelný emulátor	185
Rejstřík		205

Podrobný obsah

Předmluva		10
Poděkování		12
Úvod		13
Kapitola 01	Nastavení vývojového prostředí	15
1.1	Požadavky na operační systém	15
1.2	Získání a instalace Pythonu 2.5	16
1.2.1	Instalace Pythonu na Windows	16
1.2.2	Instalace Pythonu pro Linux	16
1.3	Příprava Eclipse a PyDev	17
1.3.1	Nejllepší přítel hackera: ctypes	19
1.3.2	Práce s dynamickými knihovnamí	19
1.3.3	Sestrojování datových typů C	21
1.3.4	Předávání parametrů odkazem	23
1.3.5	Definice struktur a unionů	23
Kapitola 02	Debuggery a jejich design	27
2.1	Registry CPU s všeobecným zaměřením	28
2.2	Zásobník	30
2.3	Ladění událostí	32
2.4	Body přerušení	33
2.4.1	Instrukční body přerušení	33
2.4.2	Hardwarové body přerušení	35
2.4.3	Paměťové body přerušení	37

Kapitola 03	Tvorba vlastního debuggeru na Windows	39
3.1	Začínáme	39
3.2	Získání stavu registru CPU	47
3.2.1	Procházení vláknů	48
3.2.2	Dejme všechno dohromady	49
3.3	Implementace zpracovatelů ladicích událostí	53
3.4	Všemohoucí bod přerušení	58
3.4.1	Instrukční body přerušení	58
3.4.2	Hardwarové body přerušení	63
3.4.3	Paměťové body přerušení	68
3.5	Závěr	72
Kapitola 04	PYDBG: debugger v Pythonu na Windows	73
4.1	Rozšiřování zpracovatelů bodů přerušení	73
4.2	Zpracovatelé porušení přístupu	76
4.3	Momentky procesu	79
4.3.1	Jak se pořídí momentka procesu	79
4.3.2	Dejme všechno dohromady	82
5.1	Instalace Immunity Debuggeru	87
Kapitola 05	Immunity Debugger: to nejlepší z obou světů	87
5.2	Immunity Debugger 101	88
5.2.1	Co jsou PyCommandy	88
5.2.2	Co jsou PyHooks	89
5.3	Vývoj exploitu	91
5.3.1	Jak najít instrukce přívětivé k exploitu	91
5.3.2	Filtrování špatných znaků	92
5.3.3	Obcházení DEP na Windows	95
5.4	Jak zmařit antiladicí rutiny v malwaru	100
5.4.1	IsDebuggerPresent	100
5.4.2	Jak zmařit iteraci přes procesy	101

Kapitola 06	Hákování	103
6.1	Měkké hákování s PyDbg	104
6.2	Tvrdé hákování s Immunity Debuggerem	108
Kapitola 07	Injectáž DLL a kódu	115
7.1	Vytvoření vzdáleného vlákna	115
7.1.1	Injectáž DLL	116
7.1.2	Injectáž kódu	119
7.2	Jdeme páchat zlo	122
7.2.1	Skrytí souboru	122
7.2.2	Kód zadních vrátek	123
7.2.3	Kompilace s py2exe	127
Kapitola 08	Fuzzing	131
8.1	Třídy chyb	132
8.1.1	Přetékání bufferů	132
8.1.2	Celočíselná přetečení	133
8.1.3	Útoky na formátovací řetězec	134
8.2	Souborový fuzzer	135
8.3	Možný rozvoj v budoucnu	142
8.3.1	Pokrytí kódu testy	143
8.3.2	Automatizovaná statická analýza	143
Kapitola 09	Framework Sulley	145
9.1	Instalace Sulley	146
9.2	Základní prvky Sulley	146
9.2.1	Řetězce	147
9.2.2	Oddělovače	147
9.2.3	Statické a znáhodněné prvky	147
9.2.4	Binární data	148
9.2.5	Celá čísla	148
9.2.6	Bloky a skupiny	149

9.3	Zavraždění WarFTPd se Sulley	150
9.3.1	FTP 101	151
9.3.2	Vytvoření kostry protokolu FTP	151
9.3.3	Relace Sulley	152
9.3.4	Monitorování sítě a procesu	154
9.3.5	Fuzzing a webové rozhraní Sulley	155
Kapitola 10	Fuzzing ovladačů Windows	159
10.1	Komunikace s ovladačem	160
10.2	Fuzzing ovladače s Immunity Debuggerem	161
10.3	Driverlib – nástroj statické analýzy pro ovladače	165
10.3.1	Odhalování názvů zařízení	165
10.3.2	Jak najdeme rutinu IOCTL dispatch	166
10.3.3	Určení podporovaných IOCTL kódů	168
10.4	Budování fuzzeru ovladače	170
Kapitola 11	IDAPython: skriptování IDA Pro	175
11.1	Instalace IDAPythonu	176
11.2	Funkce IDAPythonu	177
11.2.1	Pomocné funkce	177
11.2.2	Segmenty	177
11.2.3	Funkce	178
11.2.4	Křížové odkazy	178
11.2.5	Háky debuggeru	178
11.3	Ukázky skriptů	179
11.3.1	Nalezení nebezpečných křížových odkazů	180
11.3.2	Pokrytí funkčního kódu testy	181
11.3.3	Výpočet velikosti zásobníku	183
Kapitola 12	PyEmu: skriptovatelný emulátor	185
12.1	Instalace PyEmu	185
12.2	Přehled PyEmu	186

12.2.1	PyCPU	186
12.2.2	PyMemory	186
12.2.3	PyEmu	187
12.2.4	Spuštění	187
12.2.5	Modifikátory paměti a registrů	187
12.2.6	Zpracovatelé	188
12.3	IDAPyEmu	192
12.3.1	Emulace funkce	194
12.3.2	PEPyEmu	197
12.3.3	Packery spustitelných souborů	198
12.3.4	Packer UPX	198
12.3.5	Rozpakování UPX s PEPyEmu	199

Rejstřík

205