

# Obsah

<b>Předmluva .....</b>	<b>11</b>
<b>O autorovi.....</b>	<b>13</b>
<b>1. Přetečení zásobníku: Základy .....</b>	<b>15</b>
<b>Výzva softwarové bezpečnosti .....</b>	<b>16</b>
Software společnosti Microsoft není bezchybný .....	17
Slabá místa a spuštění vzdáleného kódu.....	18
Nárůst v přetečení zásobníku.....	20
Madonna napadena! .....	21
Definice .....	22
Hardware.....	23
Software .....	23
Bezpečnost.....	27
<b>2. Porozumění shell kódu.....</b>	<b>31</b>
Přehled kódu shellu.....	32
Nástroje.....	32
<b>Programovací jazyk assembler .....</b>	<b>33</b>
Assembler v Unixu a ve Windows .....	37
<b>Problém adresování.....</b>	<b>37</b>
Použití triku s instrukcemi „call“ a „jmp“.....	37
Přesouvání argumentů .....	38
<b>Problém bytu NULL .....</b>	<b>39</b>
<b>Implementace systémových volání.....</b>	<b>40</b>
Čísla systémových volání.....	40
Argumenty systémových volání.....	40
<b>Vzdálený kód.....</b>	<b>42</b>
Kód pro svázání shellu s portem .....	42
Kód rozdvojení popisovačů socketů .....	44
<b>Místní kód .....</b>	<b>45</b>
Kód execve .....	45
Kód setuid .....	47
Kód chroot .....	48

<b>3. Psaní shell kódu .....</b>	<b>57</b>
<b>Příklady shell kódu .....</b>	<b>58</b>
Systémové volání Write .....	60
Shell kód execve .....	64
Hodnoty „aaaabbbbcccc“ jsou ukazatele na „date“, „-c“, a „/bin/sh“ .....	69
Spuštění .....	72
Shell kód svazující shell s portem .....	72
Shell kód pro obrácené připojení .....	82
Shell kód využívající použité sockety .....	85
Využívání použitých popisovačů souborů .....	87
Zašifrování shell kódu .....	94
<b>Využití proměnných programu .....</b>	<b>99</b>
Open Source Programy .....	99
Shell kód pro více operačních systémů .....	103
Porozumění existujícímu shell kódu .....	104
<b>4. Assembler Win32 .....</b>	<b>111</b>
<b>Rozložení paměti aplikace .....</b>	<b>112</b>
Struktura aplikace .....	114
<b>Přidělování paměti – fronta .....</b>	<b>114</b>
<b>Přidělení paměti – halda .....</b>	<b>115</b>
Struktura haldy .....	116
<b>Assembler ve Windows .....</b>	<b>116</b>
Registry .....	116
Indexovací registry .....	117
Registry fronty .....	117
Další registry s obecným účelem .....	118
EIP Registr .....	118
Datové typy .....	118
Operace .....	118
Hello World .....	118
<b>5. Přetečení fronty .....</b>	<b>123</b>
<b>Architektura Intel x86 a základy strojového jazyka .....</b>	<b>125</b>
Registry .....	125
Volání zásobníku a procedur .....	127
Ukládání lokálních proměnných .....	128

<b>Volací konvence a díly fronty .....</b>	<b>133</b>
Úvod do rámce fronty .....	133
Předávání argumentů funkcí .....	134
Jděte s davem .....	140
Disassemblery pro Windows a Unix .....	140
Rámec fronty a syntaxe volání .....	142
<b>Rozložení paměti procesu .....</b>	<b>143</b>
<b>Přetečení front a jejich zneužití .....</b>	<b>144</b>
Jednoduché přetečení .....	146
Vytvoření vzorového příkladu se zneužitelným přetečením .....	150
Psaní kódu, ve kterém může dojít k přetečení .....	150
Zpětný překlad kódu s přetečením do assembleru .....	151
Provedení exploitu .....	153
Obecná koncepce zneužití .....	153
Techniky vniknutí do zásobníku .....	154
Optimalizace vpravočacího vektoru .....	154
Určení umístění těla .....	154
Metody ke spuštění těla .....	155
Přímý skok (Hádání odskoků) .....	155
Návrat naslepo .....	155
Návrat pomocí několika instrukcí Pop .....	156
Volání registru .....	156
Přesunutí návratu .....	157
Co je to odskok? .....	157
Sled instrukcí No Operation (NOP) .....	158
Návrh těla .....	158
Škoda & Obrana .....	163
Zneužití pomocí Perlu .....	163
<b>Co je přetečení Off-by-One? .....</b>	<b>163</b>
Jděte s davem .....	167
Přepsání ukazatelů vztahujících se k frontě .....	167
<b>Funkce, které mohou způsobit přetečení zásobníku .....</b>	<b>169</b>
Funkce a jejich problémy aneb nikdy nepoužívejte gets() .....	169
strcpy() a strncpy(), strcat() a strncat() .....	169
(v)sprintf() a (v)snprintf() .....	170
sscanf(), vscanf() a fscanf() .....	171
Další funkce .....	171
<b>Výzvy v hledání přetečení zásobníku .....</b>	<b>172</b>
Lexikální analýza .....	173
Sémantické analyzéry .....	175

<b>Ochrana aplikací.....</b>	<b>176</b>
OpenBSD 2.8 ftpd Off-by-One .....	176
Přetečení zásobníku v Apache httpasswd.....	177
<b>6. Přetečení haldy .....</b>	<b>185</b>
<b>Jednoduché poučení .....</b>	<b>186</b>
Použití haldy – malloc(), calloc() a realloc() .....	187
Jednoduché přetečení haldy a BSS .....	188
<b>Přetečení ukazatelů funkcí v C++.....</b>	<b>190</b>
<b>Přetečení haldy pro pokročilé – Doug Lea malloc .....</b>	<b>193</b>
Přehled Doug Lea malloc .....	193
Uspořádání paměti – hraniční značky, schránky, arény .....	194
<b>Algoritmus free() .....</b>	<b>198</b>
<b>Falešné díly .....</b>	<b>199</b>
<b>Zneužití funkce frontlink() .....</b>	<b>204</b>
Jděte s davem .....	205
Chyby dvojitého volání free().....	205
Off-by-One a Off-by-Five technika na haldě.....	205
<b>Přetečení haldy pro pokročilé – System V malloc.....</b>	<b>206</b>
Chod System V malloc .....	206
Struktura stromu .....	207
Uvolňování paměti.....	209
Funkce realloc() .....	210
Funkce t_delete–místo ke zneužití.....	213
<b>Ochrana aplikací.....</b>	<b>215</b>
Oprava chyb v zabezpečení přetečení haldy ve zdrojovém kódu .....	216
<b>7. Útoky pomocí formátovacích řetězců .....</b>	<b>223</b>
Co je to formátovací řetězec? .....	224
Funkce v C s proměnným počtem argumentů .....	224
Ellipsis a va_args .....	225
Funkce formátovacího výstupu .....	227
Škody & ochrana .....	228
Chyby zabezpečení formátování řetězce vs. přetečení zásobníku .....	228
<b>Použití formátovacích řetězců .....</b>	<b>229</b>
Příklad printf().....	229
Formátovací tokeny a argumenty funkce printf().....	230
Typy specifikátorů formátu .....	230

<b>Zneužívání formátovacích řetězců.....</b>	<b>232</b>
Hrátky se špatnými formátovacími řetězci.....	234
Odmítnutí služby .....	234
Přímý přístup k argumentům .....	235
Čtení paměti.....	235
Zápis do paměti.....	238
Jednoduché zápisy do paměti.....	238
Jděte s davem.....	240
Změna logiky programu.....	240
Více přepsání .....	241
<b>Výzvy při zneužívání chyb formátovacích řetězců .....</b>	<b>242</b>
Hledání chyb formátovacích řetězců .....	243
Jděte s davem.....	244
Více fronty za méně formátovacích řetězců .....	244
Co přepsat.....	245
Destruktory v dtors .....	245
Vstupy v tabulce globálních odskoků (GOT).....	248
Strukturované obsluhovače výjimek.....	250
<b>Rozdíly v operačních systémech .....</b>	<b>250</b>
Obtíže při zneužívání různých systémů .....	253
<b>Ochrana aplikací.....</b>	<b>253</b>
Vnitřní a vnější analýza aplikace .....	254
<b>8. Přetečení zásobníku ve Windows .....</b>	<b>259</b>
Pozadí .....	260
Základní přetečení fronty.....	260
Psaní shell kódu pro Windows .....	267
Překonání speciálních znaků (Příklad: NULL) .....	272
Aplikace klient-server .....	277
Použití či zneužití strukturovaného zpracování výjimek .....	288
<b>9. Hledání přetečení zásobníku ve zdroji.....</b>	<b>297</b>
Analýza zdrojového kódu.....	298
Nástroje zdarma Open Source .....	299
Application Defense Snapshot .....	300
RATS .....	302

<b>Flawfinder .....</b>	<b>306</b>
Textový výstup z Flawfinderu .....	307
ITS4 311	
<b>Ochrana aplikací – podnikový vývojář .....</b>	<b>311</b>
<b>Secure Software.....</b>	<b>315</b>
<b>Architektura a nasazení.....</b>	<b>316</b>
<b>Znalostní báze bezpečnostních chyb.....</b>	<b>316</b>
<b>Použití CodeAssure .....</b>	<b>318</b>
Vytváření projektů .....	319
Provádění analýzy .....	319
Posudek zranitelnosti a hlášení.....	320
Vyšetřování výsledků .....	322
Odstraňování chyb .....	323
<b>Ounce Labs .....</b>	<b>324</b>
Princip automatizované analýzy Prexis .....	324
Architektura Prexis .....	325
Schopnost ohodnocení Prexis.....	325
Schopnosti hlášení a odstraňování chyb Prexis.....	325
Prexis v akci .....	326
Ohodnocení bezpečnostních chyb s Prexis .....	327
Konfigurace projektu .....	327
Spuštění ohodnocení .....	327
Prohlídka výsledků ohodnocení .....	327
Filtrování ohodnocení.....	328
Odstraňování chyb .....	329
<b>Fortify Software .....</b>	<b>331</b>
Sada pro analýzu zdrojového kódu od Fortify .....	332
Použití mechanismu analýzy zdrojového kódu .....	332
Integrace s výrobním procesem .....	332
Průběh analýzy/výkon analýzy .....	333
Porozumění surovému výstupu.....	333
Audit Workbench .....	334
Průvodce Auditem .....	335
Manager bezpečností softwaru .....	338
<b>Rejstřík .....</b>	<b>343</b>