Obsah

1 Počítač na našem stole **8**
1.1 Mikroprocesory kompatibilní s Intel x86 9
1.1.1 Reprezentace dat 10
1.1.2 Správa paměti a překlad adres 11
1.1.3 Úrovně oprávnění 13

2 Operační systém a bezpečnost **15**
2.1 Bezpečnost na uživatelské úrovni 15
2.2 Bezpečnost na aplikační úrovni 17
2.3 Bezpečnost na úrovni jádra 18
2.4 Nízkoúrovňová bezpečnost 19
2.5 Software s otevřeným zdrojovým kódem, GNU/Linux 20
2.6 Operační systém s linuxovým jádrem 21
2.6.1 Virtuální adresní prostor 22

3 Programovací jazyky **24**

4 Základy assembleru v Linuxu a nástroje **26**
4.1 Potřebné nástroje 26
4.2 Základy assembleru 27
4.2.1 Syntaxe AT&T 27
4.2.2 Funkce jádra a knihovní funkce 29
4.2.3 Rozdíly systému FreeBSD 31
4.3 Assembler vkládaný do jazyka C 32
4.3.1 Rozšířený vkládaný assembler 33

5 Převzetí kontroly nad procesem **37**
5.1 Shellkód 39
5.1.1 Prostředí 40
5.1.2 Provedení funkce - tři kroky 44
5.1.3 Nestandardní využití registru EBP 47
5.1.4 Tvorba shellkódu 47
5.2 Buffer overflow - zápis mimo meze pole 69
5.2.1 Úvod 69
5.2.2 Cílové oblasti zápisu mimo meze 75
5.2.3 Přehled možných důsledků zápisu mimo meze 77
5.2.4 Vzorové příklady 82
5.3 Chyby při formátování řetězce 92
5.3.1 Úvod 92
5.3.2 Zápis do paměti 95
5.3.3 Využití chyby formátovacího řetězce 96
5.4 Ostatní časté chyby 102
5.4.1 Časově závislé chyby - race condition 102
5.4.2 Vytváření dočasných souborů 106
5.4.3 Nebezpečná funkce system() 108
5.4.4 Aritmetické chyby 111
5.5 Detekce chyb a obrana 113
5.5.1 Vylepšení programátorského stylu 113
5.5.2 Statická kontrola zdrojového textu 114
5.5.3 Omezené prostředí a dynamická kontrola 117

6 Útoky **124**
6.1 Počítačové viry, červi a trojské koně 124
6.1.1 Viry 126
6.1.2 Červi 147

7 Pohled do budoucnosti **152**