

Jon Erickson

# Forbidden Code

Überarbeitete Auflage

Übersetzung aus dem Amerikanischen  
von Ian Travis



# Inhaltsverzeichnis

<b>Vorwort</b> .....	7
<b>Danksagungen</b> .....	9
<b>0x100 Einleitung</b> .....	11
<b>0x200 Programmierung</b> .....	17
2.1 Was ist Programmierung? .....	18
2.2 Programme ausnutzen .....	22
2.3 Allgemeine Angriffstechniken .....	26
2.4 Dateiberechtigungen für Multiuser-Betriebssysteme .....	26
2.5 Speicher .....	28
2.6 Buffer-Overflow (Pufferüberlauf) .....	35
2.7 Stack-basierter Overflow .....	36
2.8 Heap- und BSS-basierte Overflows .....	57
2.9 Format-Strings .....	71
2.10 Shellcode programmieren .....	106
2.11 Der Rücksprung zu libc .....	158
<b>0x300 Netzwerke</b> .....	171
3.1 Was bedeutet Netzwerk? .....	171
3.2 Interessante Schichten im Detail .....	174
3.3 Netzwerke sniffen .....	179
3.4 TCP-/IP-Hijacking .....	190
3.5 Denial-of-Service .....	195
3.6 Port-Scanning .....	198

<b>0x400 Kryptologie</b> .....	211
4.1 Informationstheorie .....	212
4.2 Algorithmenlaufzeit .....	215
4.3 Symmetrische Verschlüsselung .....	217
4.4 Asymmetrische Verschlüsselung .....	219
4.5 Hybride Verschlüsselung .....	226
4.6 Passwörter cracken .....	239
4.7 802.11b-Wireless-LAN-Verschlüsselung .....	256
4.8 WEP-Angriffe .....	259
<b>0x500 Zusammenfassung</b> .....	275
<b>Stichwortverzeichnis</b> .....	279