

# Metody zapobiegania podśluchom w sieciach komputerowych

Wstęp..... 6

Rozdział 1.

Cel i zakres pracy ..... 7

1. Włamania komputerowe w świetle prawa..... 8

1.1. Przestępczość komputerowa .....11

Rozdział 2.

Metody włamań do sieci.....13

Rozdział 3.

Źródła ataków na sieci komputerowe.....13

3.2. Najczęściej stosowane technologie zabezpieczeń.....16

3.3. Port Scanning .....17

3.4. Exploit .....19

3.5. Łamanie haseł.....19

3.5.1. Metoda Brutal Force.....19

3.5.2. Metoda słownikowa .....20

3.5.3. Programy służące do łamania haseł w systemach Unix.....20

3.5.3.1. Program Fbrute.....20

3.5.3.2. Program Guess .....20

3.5.3.3. Program Killer .....20

3.5.3.4. Program John the Ripper.....21

3.5.3.5. Program Brutus .....21

3.5.3.6. Program Cracker Jack .....21

3.6. Konie trojańskie .....21

3.6.1. NetBus .....22

3.7. Spoofing .....23

## **Rozdział 4.**

### **Metody realizacji podsłuchów w sieciach.....25**

- 4.1. Adres MAC .....27
- 4.2. Sniffing aktywny.....29
- 4.3. Sniffing bierny.....30

## **Rozdział 5.**

### **Narzędzia realizacji podsłuchów.....33**

- 5.1. Pakiet dsniff.....33
  - 5.1.1. Atak Man-In-The-Middle z wykorzystaniem pakietu Dsniff .....34
  - 5.1.2. Podsłuchiwanie sesji szyfrowanych protokołem ssh .....36
  - 5.1.3. Podsłuchiwanie szyfrowanych połączeń HTTP .....36
  - 5.1.4. Atak 'pośredniczący' z wykorzystaniem pakietu Dsniff dla sieci z przełącznikami .....37
  - 5.1.5. Inne programy wchodzące w skład programu Dsniff.....39
- 5.2. Program Snort .....40
- 5.3. Program Ksniffer .....41
- 5.4. Program Sniffit 0.3.5 .....42
- 5.5. Program Ethereal.....43
- 5.6. Program Tcpdump .....44
- 5.7. Program ICMP Sniff .....44
- 5.8. Program SpyNet .....45
  - 5.8.1. CaptureNet .....46
  - 5.8.2. PeepNet .....47
- 5.9. Program Gobbler and Beholder.....48
- 5.10. Program Capsa .....49
- 5.11. Program WinSniffer (BUTTsniffer).....51
- 5.12. Program Snmpsniff .....53
- 5.13. Program WinDump .....53
- 5.14. Program SuperSniffer.....54
- 5.15. Program SerialSniffer.....54
- 5.16. Program LanChatProSniffer.....54
- 5.17. Program GnuSniff .....55

5.18.	Program SynSniff .....	55
5.19.	Program Trafdisp.....	56
5.20.	Program ANASIL .....	56
5.21.	Program ETHLOAD.....	57
5.22.	Program Netman .....	57
5.23.	Program Hunt .....	57
5.24.	Cisco Secure IDS jako sprzętowa realizacja sniffera .....	58
5.25.	Carnivore .....	58
5.26.	Projekt Eschelon.....	59
5.27.	System SORM i SORM – 2 .....	60
5.28.	Keyboard Sniffing .....	61
5.28.1.	Keyboard sniffing sprzętowy .....	61
5.28.2.	Keyboard sniffing programowy .....	61
5.29.	Emisja elektromagnetyczna .....	62

## **Rozdział 6.**

### **Metody zapobiegania podsłuchom w sieciach.....64**

6.1.	Kryptografia .....	65
6.1.1.	Szyfry wykorzystujące klucz symetryczny .....	66
6.1.1.1.	DES .....	66
6.1.1.2.	IDEA .....	69
6.1.1.3.	RC5.....	69
6.1.2.	Szyfry wykorzystujące klucz publiczny.....	69
6.1.2.1.	Algorytm Diffiego – Hellmana .....	69
6.1.2.2.	RSA.....	71
6.1.3.	DSS.....	73
6.1.4.	Szyfry hybrydowe .....	73
6.1.5.	Skróty wiadomości.....	73
6.1.5.1.	MD5 (Message Digest #5) .....	74
6.1.5.2.	SHA – 1 .....	75
6.1.5.3.	HMAC (Hashed Message Autenikation Code) .....	75
6.1.6.	Sprzętowa implementacja algorytmów szyfrujących.....	75
6.2.	SSH – Secure Shell .....	75
6.3.	PGP.....	78

6.3.1. Zasada działania PGP .....	79
6.4. SSL oraz TSL.....	87
6.5. Tunelowanie .....	93
6.6. Systemy weryfikacji autentyczności – Kerberos .....	94
6.7. Steganografia.....	98
6.8. Segmentacja sieci.....	99
6.9. IPv6 oraz IPSec .....	100
6.10. Atysniffing oraz systemy analizy ruchu pakietów w sieci.....	101
6.10.1. Cisco Secure IDS v.2.5 .....	101
6.10.2. Program Snort .....	101
6.10.3. Program L0pht AntiSniff.....	102
6.10.4. Program Neped.....	103
6.10.5. Projekt Sentinel .....	103
6.11. Interfejsy sieciowe.....	104
6.12. Systemy identyfikacji oraz haseł jednorazowych .....	105
6.12.1. Systemy identyfikacji oparte na przedmiotach .....	105
6.13.2. Systemy haseł jednorazowych (S/Key).....	107
6.14. Nośnik fizyczny jako bezpieczny sposób przekazywania danych.....	108
6.15. Fizyczny oraz logiczny nadzór nad siecią komputerową .....	108
6.16. Ochrona informacji przed emisją elektromagnetyczną .....	108
<b>Podsumowanie.....</b>	<b>111</b>
<b>Literatura .....</b>	<b>113</b>
<b>Streszczenie.....</b>	<b>115</b>