

# Obsah

<b>1</b>	<b>Bezpečnostní hrozby</b>	<b>1</b>
1.1	Vývoj počítačové bezpečnosti . . . . .	2
1.2	Druhy útoků . . . . .	2
1.2.1	Průzkum sítě . . . . .	3
1.2.2	Hromadný ping . . . . .	4
1.2.3	Odchytávání paketů . . . . .	4
1.2.4	Skenování portů . . . . .	5
1.2.5	Internetové informace . . . . .	5
1.2.6	Získání přístupu . . . . .	7
1.2.7	Využití důvěryhodnosti . . . . .	10
1.2.8	Přetečení zásobníku . . . . .	12
1.2.9	Exploit . . . . .	14
1.2.10	Phishing . . . . .	14
1.2.11	Pharming . . . . .	14
1.2.12	Útoky na webové aplikace . . . . .	15
1.2.13	SQLInjection . . . . .	18
1.2.14	Denial of service (DoS) . . . . .	20
1.2.15	Útoky pomocí ICMP zpráv . . . . .	21
1.2.16	TCP SYN Flood . . . . .	22
1.2.17	DDoS . . . . .	22
1.3	Nebezpečné programy . . . . .	23
1.3.1	Viry . . . . .	23
1.3.2	Červi . . . . .	23
1.3.3	Trojské koně . . . . .	25
<b>2</b>	<b>Cisco ASA</b>	<b>27</b>
2.1	Konfigurace . . . . .	27
2.2	Systém . . . . .	28

2.3	Instalace . . . . .	28
2.4	Základní nastavení . . . . .	29
2.5	Praktická cvičení . . . . .	30
2.5.1	Laboratorní cvičení 1 . . . . .	30
2.5.2	Laboratorní cvičení 2 . . . . .	31
<b>3</b>	<b>Zabezpečení síťových zařízení</b>	<b>33</b>
3.1	Fyzická bezpečnost . . . . .	34
3.2	Bezpečnost operačních systémů . . . . .	35
3.3	Zabezpečení samotného routeru . . . . .	35
3.3.1	Hesla . . . . .	35
<b>4</b>	<b>Autentizace, Autorizace, Accounting</b>	<b>45</b>
4.1	Autentizace . . . . .	47
4.1.1	Lokální autentizace . . . . .	48
4.1.2	Serverově orientovaná autentizace . . . . .	49
4.2	Autorizace . . . . .	49
4.2.1	Serverově orientovaná autorizace . . . . .	50
4.3	Accounting . . . . .	50
4.4	Protokoly RADIUS a TACACS+ . . . . .	53
4.4.1	Výhody protokolu RADIUS . . . . .	53
4.4.2	Výhody protokolu TACACS+ . . . . .	54
4.5	Bezpečnost vzdálené administrace . . . . .	54
4.5.1	Rizika vzdálené správy . . . . .	55
4.5.2	Ochrana AUX linky . . . . .	56
4.5.3	Omezení přístupu přes HTTP . . . . .	56
4.5.4	Omezení přístupu IP pomocí ACL . . . . .	57
4.5.5	HTTP autentizace . . . . .	57
4.5.6	Zabezpečení VTY linek . . . . .	57
4.5.7	Komunikační protokol . . . . .	58
4.6	NTP protokol . . . . .	63
4.6.1	Stratum . . . . .	64
4.6.2	Příkazy pro ovládání . . . . .	64
4.6.3	Ruční nastavení . . . . .	65
4.6.4	Centrální server . . . . .	65
4.6.5	Zařízení v roli klienta . . . . .	65
4.6.6	Zařízení v roli serveru . . . . .	65
4.6.7	Plochy model . . . . .	66

4.6.8	Hierarchický model . . . . .	66
4.6.9	Filtrování komunikace NTP . . . . .	68
4.6.10	NTP autentizace . . . . .	69
4.7	Logování . . . . .	70
4.7.1	Konzole . . . . .	71
4.7.2	Terminálové linky . . . . .	71
4.7.3	Buffered logging . . . . .	71
4.7.4	SNMP trapy . . . . .	71
4.7.5	Syslog . . . . .	72
4.7.6	Nastavení zdrojového interface . . . . .	73
4.7.7	Nastavení časových razítek logovacích zpráv . . . . .	73
4.7.8	Logování příkazů . . . . .	74
4.8	Banner . . . . .	74
4.9	Nepoužívané služby . . . . .	75
4.10	Samostudium . . . . .	76
4.11	Praktická cvičení . . . . .	78
<b>5</b>	<b>Firewall</b> . . . . .	<b>81</b>
5.1	ACL - Access Control List . . . . .	81
5.2	Typy ACL . . . . .	81
5.2.1	Port ACL . . . . .	82
5.2.2	Router ACLs . . . . .	83
5.2.3	VLAN mapy . . . . .	83
5.3	Firewall a jeho druhy . . . . .	90
5.3.1	Paketový filtr . . . . .	90
5.3.2	Circuit Gateways . . . . .	91
5.3.3	Aplikační brána . . . . .	91
5.3.4	Network Address Translation (NAT) . . . . .	91
5.4	Srovnání ASA, IOS, Windows, Linux a MacOS . . . . .	91
5.4.1	Konfigurace firewallu - Linux . . . . .	91
5.4.2	Konfigurace firewallu - MacOS . . . . .	94
5.4.3	Konfigurace firewallu - Windows . . . . .	94
5.4.4	Konfigurace firewallu - IOS . . . . .	95
5.4.5	Konfigurace firewallu - ASA . . . . .	96
5.5	Stateful paketová inspekce a Zone-based policy firewall (ZBPF) . . . . .	96
5.5.1	Stateful paketová inspekce . . . . .	97
5.5.2	Konfigurace globálních časových limitů a prahových hodnot . . . . .	98

8.5.10	VLAN hopping a DTP . . . . .	136
8.6	DHCP snooping, DAI, Source Guard . . . . .	137
8.6.1	DHCP snooping . . . . .	137
8.6.2	Dynamic ARP Inspection . . . . .	138
8.6.3	IP Source Guard . . . . .	140
8.7	Praktická cvičení . . . . .	141
8.7.1	Laboratorní cvičení 1 - konfigurace zabezpečené sítě . . . . .	141
8.7.2	Laboratorní cvičení 2 - konfigurace autentizace uživatelů . . . . .	142
8.7.3	Laboratorní cvičení 3 - konfigurace Spanning-Tree Protocol . . . . .	143
8.7.4	Laboratorní cvičení 4 - konfigurace DHCP snooping, Dynamic ARP Inspection . . . . .	144
<b>9</b>	<b>Bezpečný přenos dat . . . . .</b>	<b>147</b>
9.1	Kryptografie . . . . .	148
9.1.1	Historické metody . . . . .	149
9.2	Kryptoanalýza . . . . .	149
9.2.1	Kryptoanalytické metody (útoky na šifru) . . . . .	149
9.3	Kryptologie . . . . .	150
9.4	Celistvost a autenticita dat . . . . .	151
9.4.1	Hashovací funkce . . . . .	151
9.5	Utajení . . . . .	154
9.5.1	Šifrování . . . . .	154
9.5.2	Utajení . . . . .	157
9.5.3	Autenticita . . . . .	158
9.5.4	Utajení, autenticita a celistvost . . . . .	160
9.5.5	Elektronický podpis . . . . .	160
9.5.6	PKI . . . . .	162
9.6	VPN . . . . .	166
9.7	IPsec . . . . .	167
9.7.1	Režimy zabezpečení paketů . . . . .	168
9.7.2	IPsec protokoly . . . . .	169
9.7.3	SPI (Security Parameter Index) . . . . .	170
9.7.4	Security associations . . . . .	170
9.7.5	PFC . . . . .	172
9.7.6	Konfigurace IOS . . . . .	172
9.7.7	Konfigurace Site-to-Site VPN ASA . . . . .	176
9.7.8	SSL VPN . . . . .	180

8.5.10	VLAN hopping a DTP . . . . .	136
8.6	DHCP snooping, DAI, Source Guard . . . . .	137
8.6.1	DHCP snooping . . . . .	137
8.6.2	Dynamic ARP Inspection . . . . .	138
8.6.3	IP Source Guard . . . . .	140
8.7	Praktická cvičení . . . . .	141
8.7.1	Laboratorní cvičení 1 - konfigurace zabezpečené sítě . .	141
8.7.2	Laboratorní cvičení 2 - konfigurace autentizace uživatelů	142
8.7.3	Laboratorní cvičení 3 - konfigurace Spanning-Tree Pro- tocol . . . . .	143
8.7.4	Laboratorní cvičení 4 - konfigurace DHCP snooping, Dynamic ARP Inspection . . . . .	144
<b>9</b>	<b>Bezpečný přenos dat</b>	<b>147</b>
9.1	Kryptografie . . . . .	148
9.1.1	Historické metody . . . . .	149
9.2	Kryptoanalýza . . . . .	149
9.2.1	Kryptoanalytické metody (útoky na šifru) . . . . .	149
9.3	Kryptologie . . . . .	150
9.4	Celistvost a autenticita dat . . . . .	151
9.4.1	Hashovací funkce . . . . .	151
9.5	Utajení . . . . .	154
9.5.1	Šifrování . . . . .	154
9.5.2	Utajení . . . . .	157
9.5.3	Autenticita . . . . .	158
9.5.4	Utajení, autenticita a celistvost . . . . .	160
9.5.5	Elektronický podpis . . . . .	160
9.5.6	PKI . . . . .	162
9.6	VPN . . . . .	166
9.7	IPsec . . . . .	167
9.7.1	Režimy zabezpečení paketů . . . . .	168
9.7.2	IPsec protokoly . . . . .	169
9.7.3	SPI (Security Parameter Index) . . . . .	170
9.7.4	Security associations . . . . .	170
9.7.5	PFC . . . . .	172
9.7.6	Konfigurace IOS . . . . .	172
9.7.7	Konfigurace Site-to-Site VPN ASA . . . . .	176
9.7.8	SSL VPN . . . . .	180

9.7.9	Konfigurace AnyConnect VPN klienta na ASA v ASDM	183
9.7.10	OpenVPN	184
9.7.11	VRF-lite	185
9.8	Samostudium	187
9.9	Praktická cvičení	187
9.9.1	Laboratorní cvičení 1	187
9.9.2	Laboratorní cvičení 2	189
9.9.3	Laboratorní cvičení 3	190
<b>10</b>	<b>Bezdrátová bezpečnost</b>	<b>193</b>
10.1	Otevřená bezdrátová síť	194
10.1.1	Základní zabezpečení pomocí SSID, WEP a ověřováním MAC adresy	194
10.1.2	Hlavní nedostatky základního zabezpečení pomocí WEP	195
10.1.3	Základní zabezpečení pomocí WPA nebo WPA2 Pre-Shared Key	196
10.1.4	Rozšířené zabezpečení bezdrátových sítí	197
10.2	Bezpečnost VoIP	198
10.2.1	Speciální infrastruktura pouze pro VoIP	199
10.3	Praktická cvičení	205
10.3.1	Laboratorní cvičení 1 - konfigurace zabezpečené bezdrátové sítě	205
10.3.2	Laboratorní cvičení 2 - konfigurace zabezpečené bezdrátové sítě	206
10.3.3	Laboratorní cvičení 3 - Zabezpečení a konfigurace podnikové sítě	207
10.3.4	Laboratorní cvičení 4 - pomocný materiál prolomení WEP/WPA	208
10.3.5	Odchytávání bezdrátového provozu	209
10.3.6	Podvodné připojení k bezdrátovému přístupovému bodu	210
10.3.7	Druhy útoků na bezdrátové sítě	212
10.3.8	Útoky v režimu ARP request replay mode	213
10.3.9	Lámání WEP klíče	213