

Obsah:

1.	Přehled bezpečnostních technologií	7
1.1.	Postupy útočníků	7
1.1.1.	Obhlídka terénu.....	8
1.1.2.	Sledování	10
1.1.3.	Soupis prostředí:	11
1.1.4.	Získání přístupu	12
1.1.5.	Rozšíření oprávnění	12
1.1.6.	Vytvoření zadních vrátek; zahlázení stop	13
1.2.	Přehled nejčastějších typů útoků:	13
1.3.	Principy návrhu pro zabezpečení:	15
1.4.	Základní bezpečnostní technologie:.....	16
1.4.1.	Filtrování paketů pomocí ACL.....	16
1.4.2.	State Full Inspection (SPI).....	16
1.4.3.	NAT - překlad síťových adres	17
1.4.4.	Filtrování provozu na aplikační vrstvě	17
1.4.5.	Filtrování obsahu	18
1.4.6.	Infrastruktura veřejného klíče	18
1.4.7.	Technologie AAA	18
	Shrnutí:	18
2.	Bezpečnostní zásady.....	20
3.	Šifrování.....	27
3.1.	Ověřování autentizace, integrity a důvěrnosti (šifrování a hashovací algoritmy)	28
3.1.1.	Ověřování integrity - hash	29
3.1.2.	Ověřování důvěrnosti a autentizace - šifrování.....	31
	algoritmus AES (Advanced Encryption Standard)	31
3.1.3.	Scénáře zajištění integrity, důvěrnosti a autentizace.....	33
3.1.4.	digitální (elektronické) podpisy:	35
3.1.5.	Steganografie	36
3.2.	VPN (Virtual Private Network).....	38
3.2.1.	VPN s protokolem IPSec	39
	Shrnutí:	42
4.	Filtrování paketů - ACL	43
4.1.	ACL na zařízeních Cisco.....	43
4.1.1.	Příklad:.....	51
4.1.2.	Nejčastější chyby při návrhu ACL.....	53

4.2.	Omezení a problémy paketových filtrů	53
	Shrnutí:	58
	Kontrolní otázky:.....	58
5.	Firewally.....	60
5.1.	Demilitarizovaná zóna (DMZ):	63
5.2.	Aplikační proxy.....	65
5.3.	Návrh některých pravidel pro firewally	69
5.4.	Firewall v Linuxu	71
5.5.	Firewall ve Windows.....	75
	Shrnutí:	77
6.	Detekce vniknutí (IDS)	78
	Shrnutí:	82
7.	Ochrana hostitelského systému	83
7.1.	zabezpečení proti místním útokům	83
7.1.1.	Windows	84
7.1.2.	Linux.....	85
7.2.	odolnost proti síťovým útokům	86
7.2.1.	Windows	87
7.2.2.	Linux.....	88
7.3.	ochrana aplikací	89
	Shrnutí:	89
8.	Oddělení prostředků.....	90
8.1.	Oddělení prostředků do bezpečnostních zón.....	90
8.1.1.	Oddělení bezpečnostních zón uvnitř jednoho systému	90
8.1.2.	oddělení bezpečnostních zón na samostatné servery.....	91
8.1.3.	Rozdělení bezpečnostních zón do několika podsítí	91
8.1.4.	Rozdělení služeb mezi bezpečnostní zóny.....	92
8.2.	VLAN (Virtuální LAN).....	93
8.2.1.	Princip vytváření VLAN:	95
8.2.2.	Účel a výhody VLAN	102
8.2.3.	Typy VLAN	102
8.2.4.	Základní příkazy pro práci s VLAN a trunk linkami na zařízeních Cisco 104	
	Shrnutí	105
	Kontrolní otázky:.....	105
	Použitá literatura:.....	107
	Úvod	