

INDICE

Introduzione	1
1 Internet e le reti IP	5
1.1 Le origini	5
1.2 La filosofia	12
1.3 I servizi	15
1.4 Le modalità di accesso	20
2 Problematiche generali sulla sicurezza	29
2.1 Requisiti fondamentali di sicurezza	29
2.2 Modelli per i servizi Internet	31
2.3 Gli attacchi informatici	38
2.4 Minacce e Contromisure	41
2.5 Definire una politica di sicurezza	45
3 Vulnerabilità TCP/IP a livello rete	53
3.1 Protocolli e architetture	53
3.1.1 Modello OSI	55
3.1.2 Architettura TCP/IP	57
3.2 Il protocollo IP	59
3.2.1 Indirizzi IP.....	66
3.2.2 Modello IP Classless	71
3.2.3 Traslazione indirizzi IP	73
3.3 Debolezze del protocollo IP.....	77
3.3.1 Vulnerabilità nell'implementazione del protocollo IP	79
4 Vulnerabilità TCP/IP a livello di routing dei pacchetti	83
4.1 Consegna dei pacchetti in una rete locale	83
4.1.1 Il protocollo ARP	86
4.1.2 Debolezze del protocollo ARP	90

4.2	Instradamento di datagrammi IP	93
4.2.1	Tabelle di routing	96
4.2.2	Protocolli di routing	99
4.2.3	Protocollo BGP	105
4.3	Protocollo ICMP	108
4.4	Vulnerabilità a livello instradamento IP	111
4.4.1	Redirezione tramite messaggi ICMP.....	114
4.4.2	Aggiramento delle regole di routing	117
5	Vulnerabilità TCP/IP a livello trasporto	119
5.1	Funzionalità dei protocolli a livello trasporto	119
5.2	UDP	121
5.3	TCP	122
5.4	Debolezze dei protocolli TCP e UDP	130
5.4.1	Port Scanning	130
5.4.2	Attacchi DOS	132
5.4.3	Attacchi per sostituzione di un partecipante	137
6	Strumenti per la sicurezza dei dati	145
6.1	Requisiti di sicurezza e crittografia	145
6.1.1	Crittografia e crittoanalisi	145
6.2	Algoritmi di crittografia simmetrici.....	150
6.2.1	One-Time Pad	152
6.2.2	Principi generali di funzionamento degli algoritmi simmetrici.....	154
6.2.3	Algoritmi simmetrici: stato dell'arte.....	158
6.3	Tecniche per la codifica di messaggi lunghi	166
6.4	Algoritmi di crittografia asimmetrici	171
6.4.1	Requisiti generali di un algoritmo asimmetrico	174
6.4.2	Algoritmo RSA	176
6.4.3	Algoritmo Diffie-Hellman	182
6.5	Segnatura dei messaggi	185
6.6	Approfondimenti matematici	194
6.6.1	Operazioni in aritmetica modulo N	194
6.6.2	Uso degli operatori logici negli algoritmi di crittografia	196
6.6.3	Algoritmo di Euclide	197
7	Soluzioni per l'Autenticazione	199
7.1	Regolare l'accesso ai servizi	199
7.2	Schemi per l'autenticazione	202
7.2.1	Schema CRAM-MD5	213
7.2.2	Schema One Time Password	214
7.2.3	Autenticazione NTLM	219
7.2.4	Protocollo Kerberos Vers. 5	222
7.2.5	Standard SASL.....	226
7.2.6	Single Sign-on	227
7.3	Gestione chiavi crittografiche	230
7.3.1	Generazione e Mantenimento delle chiavi	230
7.3.2	Distribuzione delle chiavi	234
7.4	Realizzare una PKI	241
8	Controllo Accessi alla Rete	247
8.1	Accessi alla rete	247
8.2	Autenticazione degli utenti	249
8.2.1	Autenticazione PAP/CHAP	253
8.2.2	Protocollo RADIUS	255
8.3	Architettura EAP.....	260
8.3.1	Schema EAP-MD5	262
8.3.2	Schema LEAP	263
8.3.3	Schema EAP-PSK	264
8.3.4	Schema EAP-TLS	265
8.3.5	Schema EAP-TTLS.....	267
8.3.6	Schema PEAP	267
8.3.7	Schema EAP-FAST	268
8.3.8	Schema EAP-IKEv2	270
8.3.9	Schema EAP-SIM	270
8.3.10	Schema EAP-AKA	271
8.4	Assegnazione e controllo dei parametri utente	273
8.4.1	Stabilire un piano di indirizzamento IP	274
8.4.2	Protocollo DHCP	276
8.4.3	Protocollo IPCP	281
9	Sicurezza Reti Wireless	283
9.1	Problematiche di sicurezza nelle Reti Wireless	283
9.2	Lo standard IEEE 802.11	284
9.3	Vulnerabilità WEP	288
9.3.1	Decodifica gratuita dei frame	293
9.3.2	Attacchi DOS	295
9.4	Lo standard WPA	296
9.5	Vulnerabilità e misure di sicurezza delle reti IEEE 802.15	298
9.6	Vulnerabilità e misure di sicurezza delle reti IEEE 802.16	302

9.7 Vulnerabilità e misure di sicurezza delle reti IEEE 802.20	306	12.7 Remote Desktop Control	406
10 Virtual Private Network	309	13 Vulnerabilità e contromisure nella posta elettronica	409
10.1 Realizzazione di una Rete Corporate	309	13.1 SMTP	409
10.2 Protocollo GRE	314	13.1.1 Formato messaggio di posta elettronica	416
10.3 Protocollo PPTP	316	13.1.2 MIME	419
10.4 IPsec	318	13.2 Vulnerabilità SMTP	420
10.4.1 IPsec Security Association	319	13.3 POP3	425
10.4.2 Modalità di fruizione dei servizi IPsec	321	13.4 IMAP4	428
10.5 IPsec Authentication Protocol.....	322	13.5 Posta Elettronica e TLS	430
10.6 IPsec Encapsulation Security Payload Protocol	326	13.6 Soluzioni per la sicurezza dei messaggi	432
10.7 IPsec – Negoziazione di una SA	328	13.6.1 PGP	436
10.7.1 IKE	333	13.6.2 S-MIME	443
10.7.2 IPsec NAT Traversal	337	14 Vulnerabilità e contromisure nel servizio WWW	447
10.8 L2TP	339	14.1 World Wide Web	447
10.9 VPN SSL/TLS	343	14.2 Protocollo HTTP	450
10.9.1 TLS Record Protocol	347	14.3 Soluzioni per l'autenticazione con HTTP	454
10.9.2 TLS Alert Protocol	349	14.3.1 Basic Access Authentication	455
10.9.3 TLS Change Cipher Spec Protocol	350	14.3.2 Digest Access Authentication	457
10.9.4 TLS Handshake Protocol	350	14.4 Vulnerabilità Web Server	462
11 Vulnerabilità e contromisure nei servizi di supporto all'uso della rete	357	14.4.1 Bad Parsing su Web Server	464
11.1 DNS	357	14.4.2 Buffer Overflow su Web Server.....	464
11.1.1 Vulnerabilità DNS.....	363	14.4.3 Cross Site Script Attack	467
11.1.2 DNSSEC	367	14.4.4 SQL Injection su Web Server.....	469
11.2 WHOIS	369	14.5 HTTP su TLS	470
11.2.1 Vulnerabilità WHOIS.....	370	14.6 Sicurezza Client Side	471
11.3 SNMP	371	14.6.1 Vulnerabilità Client Script	471
11.4 Ident	377	14.6.2 Java	472
11.5 Finger	379	14.6.3 ActiveX	481
11.6 NTP	380	15 Sicurezza dei sistemi	483
12 Vulnerabilità e contromisure nel controllo remoto e scambio file	385	15.1 Individuazione delle risorse da proteggere	483
12.1 Telnet	385	15.2 Protezione Account e Password	490
12.2 R Command	388	15.3 Protezione del File System.....	497
12.3 RPC	389	15.4 Eliminazione servizi non necessari	500
12.4 FTP e TFTP	393	15.5 Classificazione agenti software ostili	503
12.4.1 Vulnerabilità FTP	397	15.5.1 Trojan Horse	506
12.5 SSH	399	15.5.2 Virus	507
12.6 Windows Share	404	15.5.3 Worm	510

15.5.4 Tool per attacchi di tipo DDOS	513
15.6 Attivazione Antivirus	515
15.7 Monitoring attività e rilevazione intrusioni	517
15.7.1 Analisi dei Log	521
16 Sicurezza perimetrale e firewall	525
16.1 Proteggere i sistemi da minacce esterne	525
16.2 Perimetro di una rete	528
16.3 I firewall.....	533
16.4 Network Level Firewall	538
16.5 Application Level Firewall	548
16.6 Circuit Level Firewall	552
16.7 Proxy Server, Relay Server e Reverse Proxy	554
16.8 Architetture firewall complesse	556
16.8.1 Screened Host Firewall	557
16.8.2 Screened Subnet Firewall	562
16.9 Network IDS	567
16.10 Honey pot.....	572
Indice analitico	575