

Indice

1	Introduzione	1
1.1	Premessa	1
1.2	Honeypot	1
1.2.1	Storia	1
1.2.2	Definizione	2
1.2.3	Vantaggi e Svantaggi	3
1.2.4	Principi di Funzionamento	4
1.2.5	Valore delle Honeypot	5
1.3	Honeynet	7
1.3.1	Storia	7
1.3.2	Definizione	7
1.3.3	Principi di Funzionamento	8
1.3.4	Requisiti fondamentali di una Honeynet	9
1.3.5	Valore delle Honeynet	11
1.3.6	Rischi collegati alla gestione di una Honeynet	12
1.4	Conclusioni	13
2	Honeypot e Honeynet: uno sguardo più approfondito	15
2.1	Premessa	15
2.2	Classificazione delle Honeypot per livelli di interazione	15
2.2.1	Honeypot a bassa Interazione	15
2.2.2	Honeypot a media Interazione	17
2.2.3	Honeypot ad alta Interazione	17
2.3	Prima Generazione	18
2.3.1	Data Control	19
2.3.2	Data Capture	21
2.3.3	Limiti	22
2.4	Seconda Generazione	23
2.4.1	Architettura	23
2.4.2	Data Control	24
2.4.3	Data Capture	24
2.4.4	Meccanismi di alert	25
2.5	Honeytoken	25
2.5.1	Definizione	25
2.5.2	Principi di Funzionamento	26
2.5.3	Valore	26
2.6	Conclusioni	27

3	Honeypot: descrizione di alcuni tool	29
3.1	Premessa	29
3.2	BackOfficer Friendly	29
3.2.1	Valore di BackOfficer Friendly	30
3.2.2	Principi di funzionamento	31
3.2.3	Informazioni Raccolte e Alerting Capabilities	32
3.2.4	Rischi	33
3.3	Specter	33
3.3.1	Valore di Specter	36
3.3.2	Principi di funzionamento	36
3.3.3	Informazioni Raccolte e Alerting Capabilities	37
3.3.4	Rischi	38
3.4	Honeyd	39
3.4.1	Valore di Honeyd	39
3.4.2	Principi di funzionamento	39
3.4.3	Informazioni Raccolte e Alerting Capabilities	42
3.4.4	Rischi	43
3.5	Honeypot “personalizzate”	43
3.5.1	Port-Monitoring Honeypot	43
3.5.2	Jailed environments	45
3.6	Decoy Server	47
3.6.1	Valore di Decoy Server	48
3.6.2	Principi di funzionamento	48
3.6.3	Informazioni Raccolte e Alerting Capabilities	49
3.6.4	Rischi	49
3.7	Conclusioni	50
4	Log e Network Forensic	51
4.1	Premessa	51
4.2	Caratteristiche dei log	51
4.2.1	Integrità	52
4.2.2	Time Stamping	53
4.2.3	Normalizzazione	53
4.3	Log correlation	53
4.4	Requisiti dei tool per l’acquisizione dei log	55
5	Caso di studio: Honeyd	57
5.1	Premessa	57
5.2	Honeypot Setup	57
5.2.1	Installazione e configurazione di Honeyd	57
5.2.2	Installazione e configurazione di Snort, Mysql e ACID	59
5.3	Analisi Log di Honeyd	60
5.3.1	Distribuzione attacchi per giorni e fasce orarie	60
5.3.2	Distribuzione attacchi per protocolli e porte	65
5.4	Conclusioni	74
6	Conclusioni	75
A	BackOfficer Friendly Log	81

B	File di configurazione e script utilizzati	87
B.1	Honeyd	87
B.1.1	honeyd.conf	87
B.1.2	honeydStart.sh	88
B.2	Snort	88
B.2.1	snort.conf	88
B.2.2	snortStart.sh	90
B.3	Script vari	91
B.3.1	startstop	91
B.4	ACID	91
B.4.1	acid_conf.php	91
