
DAFTAR ISI

KATA PENGANTAR.....	v
KATA PENGANTAR BUKU CYBER SECURITY:.....	vi
DAFTAR ISI	vii
DAFTAR GAMBAR.....	xvii
DAFTAR TABEL	xix
BAB I DASAR-DASAR <i>CYBER SECURITY</i>.....	1
1.1. Pendahuluan	1
1.2. Sejarah Kejahatan Cyber	2
1.3. Motivasi dan Jenis Serangan	3
1.3.1. Serangan tidak terstruktur	6
1.3.2. Serangan terstruktur	7
1.3.3. Rekayasa sosial (Phishing, Spear phishing)	7
1.3.4. Denial of Service (DoS dan DDoS).....	7
1.3.5. Man-in-the-middle attack (MITM).....	8
1.3.6. Botnet	8
1.3.7. Skrip lintas situs	9
1.3.8. Serangan download drive-by	9
1.3.9. Advanced Persistent Threat (APT).....	10
1.3.10. Serangan Basis Web.....	11
1.3.11. Serangan dari Internal	11
1.3.12. Ransomware	12
1.3.13. Spionase 12	12
1.4. Digital Forensic	13
1.4.1. Definisi komputer forensik.....	13
1.4.2. Cyber crime	14
1.5. Kesimpulan	14
1.6. Latihan.....	15

BAB II	FRAMEWORK CYBER SECURITY	17
2.1.	Pendahuluan	17
2.1.1.	Dasar keamanan informasi	17
2.1.1.1.	Autentikasi	19
2.1.1.2.	Otorisasi	21
2.1.1.3.	Nonrepudiation	22
2.1.1.4.	Confidentiality	23
2.1.1.5.	Integrity	24
2.1.1.6.	Avalaibility	25
2.2.	Kesimpulan	26
2.3.	Latihan	28
BAB III	TEKNIK DAN MOTIVASI MENYERANG	29
3.1.	Pendahuluan	29
3.1.1.	Penggunaan <i>Proxy</i>	29
3.1.1.1.	Jenis <i>Proxy</i>	31
3.1.1.2.	Mendeteksi Penggunaan <i>Proxy</i>	33
3.1.2.	Teknik <i>Tunneling</i>	34
3.1.2.1.	HTTP Akses	37
3.1.2.2.	DNS	38
3.1.2.3.	ICMP	40
3.1.2.4.	Deteksi dan penanganan	41
3.2.	Teknik Fraud	43
3.2.1.	Phishing, Smishing, Vishing, and Mobile Malicious Code	43
3.2.1.1.	Mobile Malicious code	44
3.2.1.2.	Phishing pada perangkat <i>mobile</i>	44
3.2.2.	Rogue Antivirus	48
3.2.2.1.	Mencari keuntungan dari pembayaran	50
3.2.3.	Melalui Fraud Klik	51
3.2.3.1.	Pay per click	52
3.2.3.2.	Tujuan Klik Fraud	53
3.2.3.3.	Strategi Klik Fraud dan cara mendeteksi	54
3.3.	Ancaman Pada Infrastruktur	56
3.3.1.	Botnet	56
3.3.2.	Fast flux	62
3.3.3.	Advance Fast flux	65

3.4.	Kesimpulan	68
3.5.	Latihan	69
BAB IV	PEMAHAMAN <i>HARDISK</i>, <i>STORAGE</i> DAN <i>FILE SYSTEM</i>	70
4.1.	Pendahuluan	70
4.1.1.	Cara Kerja Hardisk	70
4.1.2.	Interface Harddisk	72
4.1.2.1.	Small Computer System Interface (SCSI)	72
4.1.2.2.	Integrated Device Electronic (IDE)	73
4.1.2.3.	EIDE	73
4.1.2.4.	Fibre Channel	74
4.1.2.5.	Serial Attached SCSI (SAS)	75
4.1.2.6.	Serial ATA (SATA)	76
4.2.	Struktur Internal <i>Hard disk</i>	76
4.2.1.	Low level format	76
4.2.2.	High level format	78
4.3.	<i>File System</i> /Sistem File	80
4.3.1.	Beberapa File System Umum Digunakan	81
4.3.1.1.	FAT	81
4.3.1.2.	NTFS	81
4.3.1.3.	File system Ext2, Ext3, Ext4	82
4.3.1.4.	File system XFS	82
4.3.1.5.	File system ZFS	82
4.3.1.6.	File system BTRFS	83
4.3.2.	Jenis File System	83
4.3.2.1.	Disk file system	84
4.3.2.2.	Flash file system	84
4.3.2.3.	Tape file system	84
4.3.2.4.	Database file system	85
4.3.2.5.	Transactional file system	86
4.3.2.6.	Network file system	86
4.3.2.7.	Share disk file system	87
4.3.2.8.	Spesial file system	87
4.3.2.9.	Minimal file system/tape file system	87
4.3.2.10.	Flat file system	88

4.4.	Kesimpulan.....	89
4.5.	Latihan.....	89

BAB V JENIS SERANGAN DAN FORENSIC PADA EMAIL..... 91

5.1.	Pendahuluan	91
5.2.	Jenis layanan email.....	92
5.3.	Serangan dan Kejahatan Pada Layanan Email	95
5.3.1.	Flaming.....	95
5.3.2.	Email Spoofing.....	96
5.3.3.	Email bombing	96
5.3.4.	Email Hacking	96
5.3.5.	Email Spam.....	96
5.3.6.	Email Phishing.....	96
5.3.7.	Email fraud	96
5.4.	Privacy pada Email.....	97
5.4.1.	Masalah pada privacy email	97
5.4.2.	Tracking email.....	98
5.5.	Email Forensic.....	98
5.5.1.	Bagian penting dari forensik email.....	98
5.5.2.	Proses forensik email	101
5.5.3.	Analisis email	101
5.5.4.	Pesan singkat	103
5.6.	<i>Tools</i> untuk Forensic Email.....	104
5.6.1.	Email tracker pro	104
5.6.2.	Email tracker secara <i>online</i>	106
5.7.	Kesimpulan.....	106
5.8.	Latihan.....	107

BAB VI JENIS SERANGAN DAN METODE FORENSIK PADA WINDOWS..... 108

6.1.	Pendahuluan	108
6.1.1.	Windows Forensik.....	108
6.1.2.	Area Penting pada Windows Forensik.....	109
6.1.2.1.	Volatile information	110
6.1.2.2.	Non Volatile Information	115

6.2.	Mengembalikan File Hilang.....	117
6.2.1.	Organisasi Data pada Windows.....	117
6.2.2.	Mengembalikan file yang dihapus.....	119
6.2.3.	Mengembalikan file cache.....	119
6.2.4.	Mengambil file di lokasi HDD yang tidak terisi	119
6.3.	Hal Penting tentang Kehilangan Data	119
6.3.1.	Slack Space	120
6.3.2.	Swap Space	120
6.3.3.	Carving File.....	121
6.3.4.	Event Logs.....	123
6.4.	Kesimpulan	124
6.5.	Latihan.....	124

BAB VII JENIS SERANGAN DAN METODE FORENSIK PADA NETWORK..... 126

7.1.	Pendahuluan	126
7.2.	Network Forensic	127
7.2.1.	Bagian Host	128
7.2.2.	Bagian Node	129
7.2.3.	Perangkat Router	130
7.2.4.	Perangkat Switch.....	130
7.2.5.	Perangkat Hub	131
7.2.6.	NIC Card	132
7.3.	Informasi Forensik dari Jaringan.....	132
7.3.1.	Intrusion Detection	132
7.3.2.	Wireless Access Point	133
7.3.3.	Log Analisis	133
7.3.4.	Analisis Time Stamp	134
7.3.5.	Analisis Data	135
7.4.	<i>Tools</i> untuk Forensik.....	135
7.4.1.	Alat jaringan yang digunakan untuk forensik	136
7.4.1.1.	Network Tap	136
7.4.1.2.	Port Mirroring	137
7.4.1.3.	Modus promiscuous	137
7.4.2.	Perangkat lunak yang digunakan untuk forensik jaringan	138
7.4.2.1.	Wireshark.....	138

7.4.2.2. TCPDUMP	140
7.5. Kesimpulan.....	141
7.6. Latihan.....	142
BAB VIII JENIS SERANGAN PADA WEBSITE DAN METODE FORENSIK.....	143
8.1. Pendahuluan	143
8.2. Serangan pada Website	144
8.2.1. Spoofing.....	144
8.2.1.1. Email Spoofing.....	144
8.2.1.2. Website Spoofing	145
8.2.2. Repudiation.....	146
8.2.3. Privacy Attack	147
8.2.4. Denial of service (DoS)	149
8.2.5. Privilege Escalation	149
8.2.6. SQL Injection	150
8.2.7. Web Attack Forensic	150
8.3. Investigasi Forensik pada Serangan Website.....	151
8.3.1. Web Application Forensic	152
8.3.1.1. Analisis Awal	152
8.3.2. Web Traffic Analysis.....	154
8.3.3. Web Application Forensic Tools	155
8.3.3.1. Logparser.....	155
8.3.3.2. Eventlog Analyzer.....	156
8.3.3.3. Web Log Analyzer	157
8.3.3.4. Open Web Analytic.....	158
8.3.3.5. Webalizer	159
8.4. Kesimpulan.....	160
8.5. Latihan.....	161
BAB IX JENIS SERANGAN DAN METODE FORENSIC PADA JARINGAN WIRELESS	162
9.1. Pendahuluan	162
9.2. Wi-Fi (Wireless Fidelity 802.11).....	163
9.3. Mendeteksi WiFi Frame	164
9.3.1. Monitoring mode	164

9.3.2. Kismet	165
9.3.3. NetStumbler	166
9.3.4. PCap	167
9.3.5. AiroDump dan AirCrack	167
9.3.6. Web Wedgie	169
9.4. Wireless Security	169
9.4.1. Wireless Attack	170
9.4.1.1. Probing and Surveillance	170
9.4.1.2. Denial of Service.....	171
9.4.1.3. Spoofing.....	171
9.4.1.4. Man in the middle attack.....	171
9.5. Mendeteksi Serangan Jaringan Wireless.....	172
9.5.1. Wireless Access Monitoring	172
9.5.2. Wireless Node Monitoring	173
9.5.3. Wireless Traffic Monitoring.....	174
9.6. Wireless Intrusion Detection Monitoring.....	174
9.6.1. Wireless Snort	174
9.6.2. WIDZ	175
9.6.3. BRO.....	175
9.6.3.1. Bro Event Engine.....	175
9.6.3.2. Bro Policy Script.....	176
9.7. Kesimpulan	176
9.8. Latihan.....	177
BAB X JENIS SERANGAN DAN METODE FORENSIC PADA DEVICE MOBILE	178
10.1. Pendahuluan	178
10.2. Tantangan Mobile Forensik.....	179
10.3. Komunikasi Mobile	179
10.3.1. Wireless 802.11 atau Wifi	180
10.3.2. Bluetooth	180
10.3.3. InfraRed (IrDA).....	181
10.4. Pembuktian pada Perangkat Mobile.....	181
10.4.1. Mobile Provider Logs.....	182
10.4.2. Subscriber Identified Module (SIM).....	183
10.4.3. Mobile Logs	183

10.4.4. Mobile Contact and Called List.....	183
10.4.5. Text Message.....	183
10.4.6. Application Mobile.....	184
10.5. Proses Forensik pada Perangkat Mobile.....	184
10.5.1. Seizure 184	
10.5.2. Acquisition.....	185
10.5.3. Pengujian dan Analisis	187
10.6. Alat atau Aplikasi Mendapatkan Hasil Forensik <i>Mobile</i>	188
10.6.1. Perangkat Keras.....	188
10.6.2. <i>Software</i> atau Aplikasi.....	189
10.7. Kesimpulan.....	192
10.8. Latihan.....	193

BAB XI ANALISIS FILE LOGS DAN CRACKING PASSWORD.....

11.1. Pendahuluan	195
11.2. File Register Pada Windows	196
11.2.1. Register dan Forensik	197
11.2.1.1. Windows System Information.....	197
11.3. Event Log File pada Windows	200
11.3.1. Event Log File Format.....	200
11.3.2. Membaca Format Event Log Format.....	200
11.3.3. Menggunakan Microsoft Log Parser	201
11.3.4. Memahami User Management Log	201
11.3.5. Memahami File Windows dan Hak Akses	202
11.3.6. Audit Perubahan Kebijakan.....	202
11.4. Lokasi <i>Password</i> pada Windows.....	203
11.4.1. SAM 203	
11.4.1.1. Menghilangkan LM <i>Hash</i>	204
11.4.1.2. Relasi Serangan.....	204
11.4.2. Active Directory (AD).....	205
11.5. Aplikasi Cracker Password.....	205
11.5.1. Metode Cracker Password	206
11.5.1.1. Brute Force	206
11.5.1.2. Dictionary Search.....	206
11.5.1.3. Syllable Attack.....	207

11.5.1.4. Rule Based Attack.....	207
11.5.1.5. Hybrid Attack dan Password Guessing.....	207
11.5.1.6. Rainbow Attack	207
11.5.1.7. System Password	209
11.5.2. Tool and Aplikasi Cracker Password	210
11.5.2.1. CMOSPwd	210
11.5.2.2. ERDcommander.....	211
11.5.2.3. Office <i>Password</i> Recovery	212
11.5.2.4. Passware Kit.....	213
11.5.2.5. PDF <i>Password</i> Cracker.....	215
11.6. Kesimpulan	215
11.7. Latihan.....	216

BAB XII MEMBUAT LAPORAN INVESTIGAS

12.1. Pendahuluan	217
12.2. Persiapan Laporan	218
12.2.1. Pengumpulan Data	218
12.2.2. Analisis Hasil	219
12.2.3. Penyusunan Laporan	220
12.2.4. Menulis dan merevisi draft laporan.....	222
12.3. Bukti Saksi Ahli	222
12.3.1. Menemukan Ahli.....	223
12.3.2. Apa yang dilakukan ahli.....	224
12.3.3. Mengapa melibatkan ahli	226
12.4. Aspek legal bidang computer	226
12.4.1. Yuridiksi.....	227
12.4.2. Net neutrality	228
12.4.3. Open internet.....	229
12.5. Kesimpulan	229
12.6. Latihan.....	230

GLOSARIUM

REFERENSI.....

TENTANG PENULIS.....