

Sumário

PARTE I – INVESTIGAÇÃO DIGITAL 1

Capítulo 1 – Investigando redes de computadores 3

1. Endereçamento IP 3
2. Serviço de resolução de nome de domínio (DNS) 5
3. Tradução de endereçamento de rede (NAT) 6
4. Provedor de acesso à Internet (ISP) 8
5. Rastreamento de e-mail 8
 - 5.1. Primeiro experimento 9
 - 5.2. Segundo experimento 11
 - 5.3. Terceiro experimento 12
 - 5.4. Quarto experimento 13
6. Busca pelo responsável de um endereço IP 16
7. Busca de informações na Internet 18
8. Coleta das informações / validade jurídica 19
- Resumo 20
- Questões para revisão 20
- Referências bibliográficas 21

Capítulo 2 – Conceitos básicos de segurança da informação 23

1. Mecanismos de proteção 23
2. Políticas de Segurança da Informação (PSI) 24
3. Cultura dos usuários 24
4. Confidencialidade 25
5. Integridade 27
6. Disponibilidade 28
7. Autenticidade 29
- Resumo 29
- Questões para revisão 30
- Referências bibliográficas 30

Capítulo 3 – Softwares maliciosos (*malwares*) e ataques a sistemas 31

1. Vírus 31
2. Cavalo de Troia (*Trojan Horse*) 32
3. *Spyware* e *Adware* 33
4. *Keylogger* 34
5. *Backdoor* 37
6. *Worm* 38
7. *Bot* e *botnet* 39
8. *Rootkit* 40
9. *Ransomware* 40
10. *Sniffer* 41
11. Engenharia social e *phishing* 43

- 12. *Defacement* (Desfiguração)43
- 13. *Pharming*44
- 14. Negação de serviço (DoS – *Denial of Service*)45
- Resumo46
- Questões para revisão47
- Referências bibliográficas47

Capítulo 4 – Fundamentos do direito digital49

- 1. Crimes cibernéticos51
 - 1.1. Crime cibernético próprio ou exclusivamente cibernético53
 - 1.2. Crime cibernético impróprio ou aberto53
 - 1.3. Sujeito ativo nos crimes cibernéticos53
 - 1.4. Sujeito passivo nos crimes cibernéticos55
 - 1.5. Competência para apurar os crimes cibernéticos55
- 2. Prova de materialidade e autoria56
- 3. Conduta danosa atípica57
- 4. Lei “Carolina Dieckmann” (Lei nº 12.737/2012)57
 - 4.1. Invasão de dispositivo informático57
 - 4.2. Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública59
 - 4.3. Clonagem de cartão60
- 5. Marco civil da Internet (Lei nº 12.965/2014)60
 - 5.1. Definições60
 - 5.2. Direitos e garantias do usuário62
 - 5.3. Neutralidade da rede65
 - 5.4. Proteção aos registros, aos dados pessoais e às comunicações privadas66
 - 5.5. Guarda de registros de conexão68
 - 5.6. Guarda de registros de acesso a aplicações de Internet na provisão de conexão69
 - 5.7. Guarda de registros de acesso a aplicações de Internet na provisão de aplicações69
 - 5.8. Responsabilidade por danos decorrentes de conteúdo gerado por terceiros71
 - 5.9. Requisição judicial de registros73
 - 5.10. Controle parental74
- 6. Tipos penais mais comuns74
- Resumo76
- Questões para revisão77
- Referências bibliográficas77

Capítulo 5 – Busca, apreensão e solicitação de perícia79

- 1. Busca e apreensão79
- 2. Solicitação de perícia81
- 3. Exemplos de ofícios solicitantes85
 - 3.1. Possível estelionato86
 - 3.2. Diálogos e acessos online88

- 3.3. Invasão e pichação90
- Resumo91
- Questões para revisão92
- Referências bibliográficas92

PARTE II – ANÁLISE FORENSE – PERÍCIA DIGITAL93

Capítulo 6 – A Perícia e o perito digital95

- 1. Perícia digital95
- 2.O perito digital96
 - 2.1.Perito oficial96
 - 2.2.Perito *ad hoc*97
 - 2.3.Assistente técnico99
 - 2.4.Perito particular100
- 3. Cadeia de custódia100
- 4. Equipamento desligado x ligado101
- 5. Etapas da perícia digital102
 - 5.1. Identificação103
 - 5.2. Coleta108
 - 5.3. Exame109
 - 5.4. Análise109
 - 5.5. Resultados110
- 6. Procedimento Operacional Padrão (POP)110
- 7. Sobre os *softwares* utilizados111
- Resumo111
- Questões para revisão112
- Referências bibliográficas112

Capítulo 7 – Equipamento desligado (*Post Mortem Forensics*)113

- 1. Proteção da mídia questionada113
- 2.Duplicação forense117
- 3. Verificação de integridade123
- 4. Exame dos dados125
 - 4.1. Exame utilizando o ambiente Linux126
 - 4.2. Exame utilizando o ambiente Windows127
- 5. Análise das informações141
- Resumo141
- Questões para revisão141
- Referências bibliográficas141

Capítulo 8 – Equipamento ligado (*Live Forensics*)143

- 1. Captura de informações144
- 2. Duplicação forense149
- 3.Verificação de integridade150
- 4.Exame dos dados151
- 5. Análise das informações154

Resumo155
Questões para revisão155
Referências bibliográficas155

Capítulo 9 – Local de Internet157

- 1.Equipamentos e procedimentos157
- 2.Exame de endereços IP e nomes de domínio158
- 3.Exame de mensagem de correio eletrônico160
- 4.Exame de sítios de Internet163
- 5.Pontos críticos166

Resumo166
Questões para revisão166
Referências bibliográficas167

Capítulo 10 – Sistemas de arquivos169

1. Representação de dados170
 2. Funcionamento básico do disco rígido175
 3. Particionamento181
 4. FAT 187
 5. NTFS193
 - 6.EXT2/EXT3199
 - 7.EXT4204
 - 8.Sistemas de arquivos utilizados em mídias ópticas205
 - 8.1.ISO9660 (CDFS – *Compact Disc File System*)205
 - 8.2.Joliet207
 - 8.3.Rock Ridge208
 - 8.4.El Torito209
 - 9.Sistemas de arquivos utilizados em DVRs209
 - 9.1.DHFS210
 - 9.2.WFS210
 10. Raid212
- Resumo214

Questões para revisão215
Referências bibliográficas215

Capítulo 11 – Recuperação de dados excluídos217

- 1.Tipos de *carving*217
- 2.*Carving* baseado em cabeçalho/rodapé ou cabeçalho/tamanho máximo218
- 3.*Carving* baseado na estrutura do arquivo222
- 4.*Carving* baseado em blocos de conteúdo223
- 5.Recuperação baseada no sistema de arquivos223
- 6.*Softwares* de recuperação228
- 6.1.Photorec229
- 6.2.Foremost231
- 6.3. Revit07232

- 6.4. Recuva232
- 6.5. Tesdisk233
- 6.6. Análise da utilização dos *softwares*234
- Resumo236
- Questões para revisão236
- Referências bibliográficas237

Capítulo 12 – Recuperação de senhas239

- 1. Recuperação direta241
- 2. Ataque do dicionário245
- 3. Ataque de força bruta250
- 4. Pré-computado (*rainbow tables*)252
- 5. Considerações importantes256
- Resumo256
- Questões para revisão257
- Referências bibliográficas257

Capítulo 13 – Exames em Sistemas Linux259

- 1. Estrutura de diretórios259
- 2. Análise de registros (*Logs*)260
- 3. Vulnerabilidades e *exploits* conhecidos263
- 4. Experimento do incidente264
- Resumo267
- Questões para revisão267
- Referências bibliográficas267

Capítulo 14 – Exames em sistemas Windows269

- 1. Registro269
- 2. *Logs* de eventos273
- 3. Lixeira276
- 4. Pré-carregamento (*Prefetch*)279
- 5. *Jump Lists*281
- Resumo282
- Questões para revisão282
- Referências bibliográficas283

Capítulo 15 – Exames em telefones celulares285

- 1. Tecnologia GSM285
- 2. Preservação da evidência286
- 3. Coleta dos dados287
 - 3.1. Conexão com o dispositivo288
 - 3.2. Coleta automática288
 - 3.3. Coleta direta293
 - 3.4. Coleta manual294
- 4. Análise das informações295

Resumo299
Questões para revisão299
Referências bibliográficas300

Capítulo 16 – Exames em dados trafegados pela rede301

1. Captura de tráfego301
2. Análise de tráfego303
3. Utilização de *framework*306
Resumo309
Questões para revisão309
Referências bibliográficas310

Capítulo 17 – Exames em DVRs (*Digital Video Recorders*)311

1. Circuito fechado de televisão (CFTV)312
2. Codificação de vídeo313
3. Funcionamento de um DVR315
4. Procedimentos de análise de um DVR317
5. Análise de DVR “genérico”319
6. Análise de DVR Vid8321
7. Análise de DVR Intelbras326
8. Análise de DVR Alive335
9. Análise de DVR Voyager339
10. Análise de DVR Seco342
Resumo345
Questões para revisão345
Referências bibliográficas346

Capítulo 18 – Engenharia reversa347

1. Aplicações da engenharia reversa347
1.1. Análise de *malwares*347
1.2. Reversão de algoritmos criptográficos348
1.3. Gerenciamento de direitos autorais348
1.4. Auditoria de *softwares*349
2. Análise estática349
2.1. Análise estática básica350
2.2. Análise estática avançada353
3. Análise Dinâmica359
3.1. Análise dinâmica básica359
3.2. Análise dinâmica avançada362
4. *Patching*363
5. Análise de código malicioso364
6. Ofuscação de código e *antidebugging*366
7. Compactadores de código (*packers*)368
Resumo369
Questões para revisão370

Referências bibliográficas370

Capítulo 19 – Laudo pericial371

- 1.Preâmbulo372
- 2.Histórico (opcional)373
- 3.Objetivo373
- 4.Material374
- 5.Exame375
- 6.Considerações técnico-periciais (opcional)377
- 7.Conclusão / Resposta aos quesitos377
- 8.Anexos378
- 9.Considerações finais379
- 10. Tópicos a serem observados381
- 11. Outros documentos382
- Resumo382
- Questões para revisão383
- Referências bibliográficas383

Capítulo 20 – Antiforenses digitais385

- 1.Destruição386
 - 1.1.Destruição física386
 - 1.2.Destruição lógica387
- 2. Ocultação389
 - 2.1.Esteganografia389
 - 2.2.*Slackering*394
 - 2.3.ADS (*Alternate Data Stream*)394
 - 2.4.Partições ocultas (HPA/DCO)396
- 3. Proteção398
 - 3.1.Criptografia tradicional398
 - 3.2.Criptografia de chave única399
 - 3.3.Criptografia de chave pública402
- Resumo402
- Questões para revisão403
- Referências bibliográficas403