INTRODUÇÃO À ANÁLISE FORENSE EM REDES DE COMPUTADORES

CONCEITOS, TÉCNICAS E FERRAMENTAS
PARA "GRAMPOS DIGITAIS"

Ricardo Kléber M. Galvão

Novatec

Editor: Rubens Prates
Capa: Carolina Kuwabata/Ricardo Kleber Galvão
Revisão gramatical: Marta Almeida de Sá
Editoração eletrônica: Carolina Kuwabata

ISBN: 978-85-7522-307-9

Histórico de impressões:

Novembro/2013 Primeira edição

Novatec Editora Ltda.
Rua Luís Antônio dos Santos 110
02460-000 – São Paulo, SP – Brasil
Tel.: +55 11 2959-6529
Fax: +55 11 2950-8869
Email: novatec@novatec.com.br
Site: www.novatec.com.br
Twitter: twitter.com/novateceditora
Facebook: facebook.com/novatec
LinkedIn: linkedin.com/in/novatec
MP20131106

Sumário

Agradecimentos **11**

Sobre o autor **13**

Prefácio **15**

Importante 18
Convenções usadas neste livro 18

Capítulo 1 ■ Computação forense **19**

1.1 Principais conceitos relacionados à computação forense 19
1.1.1 Terminologia 20
1.1.2 Perícias públicas e privadas 22
1.1.3 Sistematização de procedimentos periciais 22
1.2 Análise forense computacional em mídias 24
1.3 Análise forense em redes de computadores (network forensics) 24
1.3.1 Questões iniciais 25
1.3.2 Questões a considerar durante a realização de perícias em redes 26
1.3.3 Objetos da análise nas perícias em redes de computadores 28
1.3.4 Desafios da análise forense em redes de computadores 29

Capítulo 2 ■ Redes de computadores **31**

2.1 Breve histórico 31
2.2 Estrutura de camadas (pilha TCP/IP) 33
2.3 Principais protocolos das camadas inferiores 34
2.3.1 Protocolo ARP 34
2.3.2 Protocolo RARP 37
2.3.3 Protocolo ICMP 38
2.3.4 Protocolo IP 41
2.3.5 Protocolo UDP 43
2.3.6 Protocolo TCP 44

2.4 Principais protocolos da camada de aplicação....46
2.4.1 Protocolo HTTP....46
2.4.2 Protocolo SMTP....48
2.4.3 Protocolos POP e IMAP....50
2.4.4 Protocolo FTP....52
2.4.5 Estruturas de outros protocolos importantes da camada de aplicação....53
2.4.6 Ferramentas para análise de protocolos de alto nível....54

Capítulo 3 ■ Captura de tráfego em redes de computadores (sniffing)....59

3.1 Sniffers: principais conceitos e técnicas envolvidas....59
3.1.1 Modo promíscuo x modo monitor....63
3.1.2 Formatos de captura: texto pleno / padrão pcap....64
3.2 Identificação de ponto de captura (instalação do "grampo digital")....64
3.2.1 Captura de tráfego em redes em barra....65
3.2.2 Captura de tráfego através de portas de monitoramento....66
3.2.3 Captura de tráfego através de interceptação intermediária....67
3.2.4 Captura de tráfego em redes sem fio (wireless)....68
3.3 Funcionamento do "grampo digital"....68
3.3.1 As bibliotecas libpcap/WinPcap e AirPcap....69
3.3.2 O tcpdump/WinDump....70
3.3.3 Limitações do tcpdump....72
3.3.4 Utilizando o tcpdump....73
3.3.5 Otimizando a captura com aplicação de filtros/parâmetros adequados....77
3.3.6 Manipulando arquivos de captura muito grandes....78
3.3.7 Conjunto de ferramentas aircrack-ng....78

Capítulo 4 ■ Análise de pacotes em redes de computadores....81

4.1 Características de comunicação (identificação de tráfego)....81
4.2 Técnicas para análise de pacotes....82
4.2.1 Pattern matching....83
4.2.2 Parsing protocol fields....85
4.2.3 Filtragem de pacotes....85
4.2.4 Técnicas para análise de protocolos de alto nível....86
4.3 Principais ferramentas para análise de tráfego de rede....87
4.3.1 Utilizando o Wireshark....87
4.3.2 Utilizando ferramentas complementares do Wireshark....92
4.3.3 Filtros (display filters) das ferramentas Wireshark/Tshark....97
4.3.4 Editores hexadecimais (hex editors)....101

4.4 Técnicas e ferramentas para reconstrução de sessões 103
4.4.1 Reconstruindo sessões com Chaosreader 104
4.5 Recuperação de arquivos trafegados em rede 105
4.5.1 Recuperando arquivos com tcpxtract 106
4.6 Protocolos inseguros (extração de informações críticas) 108
Captura de tráfego FTP 108
Captura de tráfego Telnet 109
Captura de tráfego POP3 110
4.7 Captura e análise de tráfego de voz sobre IP (VoIP) 111
4.7.1 Explorando a vulnerabilidade rtp playback 111
4.7.2 Capturando e descobrindo dados de autenticação SIP 113
4.8 Captura e análise de tráfego de serviços de comunicação e redes sociais 115
4.8.1 Serviços de comunicação com acesso a partir de portas específicas 115
4.8.2 Serviços de comunicação com acesso a partir de portas não específicas 116
4.8.3 Captura/análise de tráfego de acesso a redes sociais 118

Capítulo 5 ■ Criptografia aplicada aos protocolos de rede 123

5.1 Alternativas aos protocolos tradicionais vulneráveis à captura 123
5.2 Criptografia na associação às redes sem fio (WEP/WPA) 124
5.3 Técnicas de quebra de criptografia WEP/WPA 126
5.3.1 Descoberta de chaves WEP compartilhadas 126
5.3.2 Descoberta de chaves WPA compartilhadas 129

Capítulo 6 ■ Frameworks para análise forense em redes de computadores 133

6.1 Captura, análise e recuperação de dados com Xplico 133

Capítulo 7 ■ Validação de tráfego de redes como prova em perícias 141

Capítulo 8 ■ Estudos de caso 143

8.1 Caso 1 – Análise de tráfego web (conteúdo) 143
8.1.1 Captura de tráfego 144
8.1.2 Análise 144
8.1.3 Resposta aos quesitos 147
8.1.4 Dados complementares da análise 148
8.2 Caso 2 – Análise de tráfego web (credenciais) 148
8.2.1 Captura de tráfego 149
8.2.2 Análise 149
8.2.3 Resposta aos quesitos 151
8.2.4 Dados complementares da análise 151