WIRESHARK

PARA PROFISSIONAIS DE SEGURANÇA

Usando Wireshark e o Metasploit Framework

Jessey Bullock • Jeff T. Parker

Novatec

Editor: Rubens Prates
Tradução: Lúcia A. Kinoshita
Revisão gramatical: Marta Almeida de Sá
Editoração eletrônica: Carolina Kuwabata

ISBN: 978-85-7522-593-6

Histórico de impressões:

Julho/2017 Primeira edição

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

Sumário

Sobre os autores 13

Sobre o revisor técnico 15

Agradecimentos 16

Introdução 17

Capítulo 1 ▪ Introdução ao Wireshark 22

O que é o Wireshark? 22
- Qual a melhor hora para usar o Wireshark? 23
- Evitando se sentir apreensivo 24

Interface de usuário do Wireshark 25
- Painel Packet List 27
- Painel Packet Details 28
- Painel Packet Bytes 30

Filtros 31
- Filtros de captura 32
- Filtros de exibição 36

Resumo 41

Exercícios 42

Capítulo 2 ▪ Configurando o laboratório 43

Kali Linux 44

Virtualização 46
- Terminologia e conceitos básicos 47
- Vantagens da virtualização 48

VirtualBox 49
- Instalando o VirtualBox 49
- Instalando o VirtualBox Extension Pack 56
- Criando uma máquina virtual Kali Linux 58
- Instalando o Kali Linux 66

W4SP Lab 72
Requisitos 72
Algumas palavras sobre o Docker 73
O que é o GitHub? 75
Criando o usuário do laboratório 76
Instalando o W4SP Lab na máquina virtual Kali 77
Configurando o W4SP Lab 80
A rede do Lab 81
Resumo 83
Exercícios 83

Capítulo 3 ▪ Conceitos básicos 85

Redes 86
As camadas do modelo OSI 86
Rede entre máquinas virtuais 90
Segurança 92
A tríade de segurança 92
Sistemas para detecção e prevenção de invasão 93
Falso-positivos e falso-negativos 94
Malware 94
Spoofing e envenenamento 96
Análise de pacotes e protocolos 97
Uma história sobre análise de protocolo 98
Portas e protocolos 102
Resumo 105
Exercícios 106

Capítulo 4 ▪ Capturando pacotes 107

Sniffing 108
Modo promíscuo 108
Iniciando a primeira captura 110
TShark 114
Lidando com a rede 119
Máquina local 120
Sniffing no localhost 122
Sniffing nas interfaces de máquinas virtuais 126
Sniffing com hubs 130
Portas SPAN 133
Taps de rede 136
Bridges Linux transparentes 138
Redes wireless 141

Carregando e salvando arquivos de captura 144
Formatos de arquivo 144
Buffers circulares e vários arquivos 148
Arquivos de captura recentes 153
Dissecadores 155
W4SP Lab: administrando tráfego HTTP não padrão 156
Filtrando nomes de arquivo no SMB 158
Atribuição de cores aos pacotes 162
Visualizando capturas de outras pessoas 165
Resumo 166
Exercícios 167

Capítulo 5 ▪ Diagnosticando ataques 169

Tipo de ataque: man-in-the-middle 170
Por que os ataques MitM são eficazes 171
Como são conduzidos os ataques MitM: ARP 171
W4SP Lab: conduzindo um ataque MitM com ARP 174
W4SP Lab: conduzindo um ataque MitM com DNS 181
Como evitar ataques MitM 189
Tipos de ataque: negação de serviço 190
Por que os ataques de DoS são eficazes 191
Como são conduzidos os ataques de DoS 192
Como evitar ataques de DoS 198
Tipos de ataque: Advanced Persistent Threat 199
Por que os ataques de APT são eficazes 200
Como são conduzidos os ataques de APT 200
Exemplo de tráfego de APT no Wireshark 201
Como evitar ataques de APT 206
Resumo 206
Exercícios 207

Capítulo 6 ▪ Wireshark para ataques 208

Metodologia de ataque 208
Reconhecimento com o Wireshark 211
Evasão de IPS/IDS 213
Splicing e fragmentação de sessão 214
Atuando para o host, e não para o IDS 215
Encobrindo as pegadas e instalando backdoors 215
Exploração de vulnerabilidades 216
Configurando o W4SP Lab com o Metasploitable 217

Iniciando o console do Metasploit 218
Exploit para VSFTP 218
Depurando com o Wireshark 220
Shell no Wireshark 222
Stream TCP exibindo um bind shell 224
Stream TCP mostrando um shell reverso 231
Iniciando o ELK 237
Captura remota por meio de SSH 239
Resumo 241
Exercícios 241

Capítulo 7 ▪ Descriptografando TLS, capturando USB, keyloggers e gráficos de rede 242

Descriptografando SSL/TLS 242
Descriptografando SSL/TLS usando chaves privadas 244
Descriptografando SSL/TLS usando chaves de sessão 249
USB e o Wireshark 252
Capturando tráfego de USB no Linux 254
Capturando tráfego de USB no Windows 257
Keylogger com o TShark 259
Gráficos de rede 263
Lua e a biblioteca Graphviz 264
Resumo 271
Exercícios 271

Capítulo 8 ▪ Scripting com Lua 272

Por que Lua? 272
Básico sobre scripting 274
Variáveis 276
Funções e blocos 278
Laços 280
Condicionais 282
Configuração 283
Verificando se há suporte para Lua 283
Inicialização de Lua 284
Configuração no Windows 285
Configuração no Linux 285
Ferramentas 286
Hello World com TShark 289
Script para contagem de pacotes 290
Script para cache ARP 295

Criando dissecadores para o Wireshark 298
Tipos de dissecadores 298
Por que um dissecador é necessário 299
Faça experimentos 309
Estendendo o Wireshark 310
Script para direção de pacotes 310
Script para marcar um pacote suspeito 313
Espiando transferências de arquivos SMB 316
Resumo 319