

目录	
对本书的赞誉	
序一	
序二	
序三	
前言	
第 1 章 通向智能安全的旅程	1
1.1 人工智能、机器学习与深度学习	1
1.2 人工智能的发展	2
1.3 国内外网络安全形势	3
1.4 人工智能在安全领域的应用	5
1.5 算法和数据的辩证关系	9
1.6 本章小结	9
参考资源	10
第 2 章 打造机器学习工具箱	11
2.1 Python 在机器学习领域的优势	11
2.1.1 NumPy	11
2.1.2 SciPy	15
2.1.3 NLTK	16
2.1.4 Scikit-Learn	17
2.2 TensorFlow 简介与环境搭建	18
2.3 本章小结	19
参考资源	20
第 3 章 机器学习概述	21
3.1 机器学习基本概念	21
3.2 数据集	22
3.2.1 KDD 99 数据	22
3.2.2 DATASET CSIC 2010	26
3.2.3 SEA 数据集	26
3.2.4 ADFA-LD 数据集	27
3.2.5 Alexa 域名数据	29
3.2.6 Scikit-Learn 数据集	29
3.2.7 MNIST 数据集	30
3.2.8 Movie Review Data	31
3.2.9 SpamBase 数据集	32
3.2.10 Enron 数据集	33
3.3 特征提取	35
3.3.1 数字型特征提取	35
3.3.2 文本型特征提取	36
3.3.3 数据读取	37
3.4 效果验证	38
3.5 本章小结	40
参考资源	40
第 4 章 Web 安全基础	41

4.1 XSS 攻击概述	41
4.1.1 XSS 的分类	43
4.1.2 XSS 特殊攻击方式	48
4.1.3 XSS 平台简介	50
4.1.4 近年典型 XSS 攻击事件分析	51
4.2 SQL 注入概述	53
4.2.1 常见 SQL 注入攻击	54
4.2.2 常见 SQL 注入攻击载荷	55
4.2.3 SQL 常见工具	56
4.2.4 近年典型 SQL 注入事件分析	60
4.3 WebShell 概述	63
4.3.1 WebShell 功能	64
4.3.2 常见 WebShell	64
4.4 僵尸网络概述	67
4.4.1 僵尸网络的危害	68
4.4.2 近年典型僵尸网络攻击事件分析	69
4.5 本章小结	72
参考资源	72
第 5 章 K 近邻算法	74
5.1 K 近邻算法概述	74
5.2 示例：hello world！K 近邻	75
5.3 示例：使用 K 近邻算法检测异常操作（一）	76
5.4 示例：使用 K 近邻算法检测异常操作（二）	80
5.5 示例：使用 K 近邻算法检测 Rootkit	81
5.6 示例：使用 K 近邻算法检测 WebShell	83
5.7 本章小结	85
参考资源	86
第 6 章 决策树与随机森林算法	87
6.1 决策树算法概述	87
6.2 示例：hello world！决策树	88
6.3 示例：使用决策树算法检测 POP3 暴力破解	89
6.4 示例：使用决策树算法检测 FTP 暴力破解	91
6.5 随机森林算法概述	93
6.6 示例：hello world！随机森林	93
6.7 示例：使用随机森林算法检测 FTP 暴力破解	95
6.8 本章小结	96
参考资源	96
第 7 章 朴素贝叶斯算法	97
7.1 朴素贝叶斯算法概述	97
7.2 示例：hello world！朴素贝叶斯	98
7.3 示例：检测异常操作	99
7.4 示例：检测 WebShell（一）	100
7.5 示例：检测 WebShell（二）	102
7.6 示例：检测 DGA 域名	103

7.7 示例：检测针对 Apache 的 DDoS 攻击	104
7.8 示例：识别验证码	107
7.9 本章小结	108
参考资源	108
第 8 章 逻辑回归算法	109
8.1 逻辑回归算法概述	109
8.2 示例：hello world！逻辑回归	110
8.3 示例：使用逻辑回归算法检测 Java 溢出攻击	111
8.4 示例：识别验证码	113
8.5 本章小结	114
参考资源	114
第 9 章 支持向量机算法	115
9.1 支持向量机算法概述	115
9.2 示例：hello world！支持向量机	118
9.3 示例：使用支持向量机算法识别 XSS	120
9.4 示例：使用支持向量机算法区分僵尸网络 DGA 家族	124
9.4.1 数据搜集和数据清洗	124
9.4.2 特征化	125
9.4.3 模型验证	129
9.5 本章小结	130
参考资源	130
第 10 章 K-Means 与 DBSCAN 算法	131
10.1 K-Means 算法概述	131
10.2 示例：hello world！K-Means	132
10.3 示例：使用 K-Means 算法检测 DGA 域名	133
10.4 DBSCAN 算法概述	135
10.5 示例：hello world！DBSCAN	135
10.6 本章小结	137
参考资源	137
第 11 章 Apriori 与 FP-growth 算法	138
11.1 Apriori 算法概述	138
11.2 示例：hello world！Apriori	140
11.3 示例：使用 Apriori 算法挖掘 XSS 相关参数	141
11.4 FP-growth 算法概述	143
11.5 示例：hello world！FP-growth	144
11.6 示例：使用 FP-growth 算法挖掘疑似僵尸主机	145
11.7 本章小结	146
参考资源	146
第 12 章 隐式马尔可夫算法	147
12.1 隐式马尔可夫算法概述	147
12.2 hello world！隐式马尔可夫	148
12.3 示例：使用隐式马尔可夫算法识别 XSS 攻击（一）	150
12.4 示例：使用隐式马尔可夫算法识别 XSS 攻击（二）	153
12.5 示例：使用隐式马尔可夫算法识别 DGA 域名	159

12.6 本章小结	162
参考资源	162
第 13 章 图算法与知识图谱	163
13.1 图算法概述	163
13.2 示例：hello world！有向图	164
13.3 示例：使用有向图识别 WebShell	169
13.4 示例：使用有向图识别僵尸网络	173
13.5 知识图谱概述	176
13.6 示例：知识图谱在风控领域的应用	177
13.6.1 检测疑似账号被盗	178
13.6.2 检测疑似撞库攻击	179
13.6.3 检测疑似刷单	181
13.7 示例：知识图谱在威胁情报领域的应用	183
13.7.1 挖掘后门文件潜在联系	184
13.7.2 挖掘域名潜在联系	185
13.8 本章小结	187
参考资源	187
第 14 章 神经网络算法	188
14.1 神经网络算法概述	188
14.2 示例：hello world！神经网络	190
14.3 示例：使用神经网络算法识别验证码	190
14.4 示例：使用神经网络算法检测 Java 溢出攻击	191
14.5 本章小结	193
参考资源	194
第 15 章 多层感知机与 DNN 算法	195
15.1 神经网络与深度学习	195
15.2 TensorFlow 编程模型	196
15.2.1 操作	197
15.2.2 张量	197
15.2.3 变量	198
15.2.4 会话	198
15.3 TensorFlow 的运行模式	198
15.4 示例：在 TensorFlow 下识别验证码（一）	199
15.5 示例：在 TensorFlow 下识别验证码（二）	202
15.6 示例：在 TensorFlow 下识别验证码（三）	205
15.7 示例：在 TensorFlow 下识别垃圾邮件（一）	207
15.8 示例：在 TensorFlow 下识别垃圾邮件（二）	209
15.9 本章小结	210
参考资源	210
第 16 章 循环神经网络算法	212
16.1 循环神经网络算法概述	212
16.2 示例：识别验证码	213
16.3 示例：识别恶意评论	216
16.4 示例：生成城市名称	220

16.5 示例：识别 WebShell 222

16.6 示例：生成常用密码 225

16.7 示例：识别异常操作 227

16.8 本章小结 230

参考资源 230

第 17 章 卷积神经网络算法 231

17.1 卷积神经网络算法概述 231

17.2 示例：hello world！卷积神经网络 234

17.3 示例：识别恶意评论 235

17.4 示例：识别垃圾邮件 237

17.5 本章小结 240

参考资源 242