

TABLE OF CONTENTS

Cloning Virtual Machine	52
Downloading Windows Targets	54
Downloading Linux Targets	56
Attacking WordPress and other applications	56

Chapter 4 . Information Gathering

Introduction	63
Service enumeration	63
Determining the network range	65
Identifying active machines	67
Finding open ports	68
Operating system fingerprinting	71
Service fingerprinting	72
Threat assessment with Maltego	73
Mapping the network	78

Chapter 5 . Vulnerability Assessment

Introduction	85
Installing, configuring, and starting Nessus	85
Nessus – finding local vulnerabilities	88
Nessus – finding network vulnerabilities	90
Nessus – finding linux-specific vulnerabilities	95
Nessus – finding Windows-specific vulnerabilities	99
Installing, configuring, and starting OpenVAS	102
Settings up an SSH Script to start OpenVAS	105
Using the OpenVAS Desktop	107
OpenVAS – finding local vulnerabilities	107
OpenVAS – finding network vulnerabilities	112
OpenVAS – finding Linux-specific vulnerabilities	116
OpenVAS – finding Window-specific vulnerabilities	120

Chapter 6 . Exploiting Vulnerabilities

Introduction	127
--------------	-----

TABLE OF CONTENTS

Preface

Chapter 1 . Up and Running with Kali Linux

Introduction	
Installing to a hard disk drive	
Installing to a USB drive with persistent memory	
Installing in VirtualBox	
Installing VMWare Tools	
Fixing the splash screen	
Starting network services	
Setting up the wireless network	

Chapter 2 . Customizing BackTrack

Introduction	
Preparing kernel headers	
Installing Broadcom drivers	
Installing and configuration ATI video card drivers	
Installing and configuration NVIDIA video card drivers	
Applying updates and configuring extra security tools	
Setting up ProxyChains	
Directory encryption	

Chapter 3 . Advanced Testing Lab

Introduction	
Getting comfortable with VirtualBox	

TABLE OF CONTENTS

Installing and configuring Metasploitable	
Mastering Armitage – the graphical management tool for Met	
Mastering the Metasploit Console (MSFCONSOLE)	
Mastering the Metasploit CLI (MSFCLI)	
Mastering Meterpreter	
Metasploitable MySQL	
Metasploitable PostgreSQL	
Metasploitable Tomcat	
Metasploitable PDF	
Implementing the browser_autopwn module	

Chapter 7 . Privilege Escalation

Introduction	
Using impersonating tokens	
Local privilege escalation attack	
Mastering the Social-Engineering Toolkit (SET)	
Delivering your payload to the victim	
Collecting victim's data	
Cleaning up the tracks	
Creating a persistent backdoor	
Man-in-the-middle attack (MITM)	

Chapter 8 . Password Attacks

Introduction	
Online Password Attacks	
Cracking HTTP Passwords	
Gaining Router Access	
Password Profiling	
Cracking a Windows password using John the Ripper	
Using dictionary attacks	
Using Rainbow Tables	
Using nVidia Compute Unified Device Architecture (CUDA)	

TABLE OF CONTENTS

Using ATI Stream	
Physical access attacks	

Chapter 9 . Wireless Attack

Introduction	
Wireless network WEP cracking	
Wireless Network WPA/WPA2 Cracking	
Automating Wireless Network Cracking	
Accessing Clients using a fake AP	
URL Traffic Manipulation	
Port Redirection	
Sniffing Network traffic	