








Mapping SEED Labs to Textbook Chapters

The SEED labs work well with most textbooks. To help instructors decide which labs to use, we have mapped our SEED labs to the chapters of several security textbooks. The mappings are conducted on the following seven textbooks. As new textbooks, new editions, and new labs become available in the future, we will update this document accordingly.

Book Title	Ed.	Year	Authors	Cover
<i>Computer Security: Principles and Practice</i>	2 nd	2012	William Stallings and Lawrie Brown	
<i>Introduction to Computer Security</i>	1 st	2011	Michael T. Goodrich and Roberto Tamassia	
<i>Computer Security</i>	3 rd	2011	Dieter Gollmann	
<i>Security in Computing</i>	4 th	2006	Charles P. Pfleeger and Shari Lawrence Pfleeger	
<i>Introduction to Computer Security</i>	1 st	2004	Matt Bishop	
<i>Computer Security: Art and Science</i>	1 st	2002	Matt Bishop	
<i>Network Security: Private Communication in a Public World</i>	2 nd	2002	Charlie Kaufman, Radia Perlman, and Mike Speciner	

Mapping SEED Labs to Textbook Chapters

Computer Security: Principles and Practice, 2nd ed.
 William Stallings & Lawrie Brown
 Prentice Hall, 2012



Types	Labs	Time (week)	Chapters
Vulnerability and Attack Labs (Linux-based)	Buffer Overflow Vulnerability	1	10
	Return-to-libc Attack	1	10
	Format String Vulnerability	1	11
	Race Condition Vulnerability	1	11
	Set-UID Program Vulnerability	1	11
	Chroot Sandbox Vulnerability	1	12
	Cross-Site Request Forgery Attack	1	-
	Cross-Site Scripting Attack	1	-
	SQL Injection Attack	1	5
	ClickJacking Attack	1	-
	TCP/IP Attacks	2	7, 22
	DNS Pharming Attacks	2	22
Exploration Labs (Linux-based)	Pack Sniffing & Spoofing	1	22
	Pluggable Authentication Module	1	3
	Web Access Control	1	-
	SYN Cookie	1	7, 22
	Linux Capability	1	4, 12
	Secret-Key Encryption	1	20
	One-Way Hash Function	1	21
	Public-Key Infrastructure	1	21, 23
Design and Implementation Labs	Virtual Private Network (Linux)	4	22
	IPSec (Minix)	4	22
	Firewall (Linux)	2	9
	Firewall (Minix)	2	9
	Role-Based Access Control (Minix)	4	4
	Capability-Based Access Control (Minix)	3	4
	Encrypted File System (Minix)	4	12
	Address Space Randomization (Minix)	2	12
	Set-RandomUID Sandbox (Minix)	1	12

Mapping SEED Labs to Textbook Chapters

Introduction Computer Security
 Michael T. Goodrich & Roberto Tamassia
 Addison-Wesley, 2011



Types	Labs	Time (week)	Chapters
Vulnerability and Attack Labs (Linux-based)	Buffer Overflow Vulnerability	1	3
	Return-to-libc Attack	1	3
	Format String Vulnerability	1	3
	Race Condition Vulnerability	1	3
	Set-UID Program Vulnerability	1	3
	Chroot Sandbox Vulnerability	1	12
	Cross-Site Request Forgery Attack	1	7
	Cross-Site Scripting Attack	1	7
	SQL Injection Attack	1	7
	ClickJacking Attack	1	7
	TCP/IP Attacks	2	5
	DNS Pharming Attacks	2	6
Exploration Labs (Linux-based)	Pack Sniffing & Spoofing	1	5
	Pluggable Authentication Module	1	3
	Web Access Control	1	7
	SYN Cookie	1	5
	Linux Capability	1	3
	Secret-Key Encryption	1	8
	One-Way Hash Function	1	8
	Public-Key Infrastructure	1	8
Design and Implementation Labs	Virtual Private Network (Linux)	4	6
	IPSec (Minix)	4	6
	Firewall (Linux)	2	6
	Firewall (Minix)	2	6
	Role-Based Access Control (Minix)	4	9
	Capability-Based Access Control (Minix)	3	3
	Encrypted File System (Minix)	4	9
	Address Space Randomization (Minix)	2	-
	Set-RandomUID Sandbox (Minix)	1	13

Mapping SEED Labs to Textbook Chapters

Computer Security, 3rd edition
Dieter Gollmann
Wiley, 2011



Types	Labs	Time (week)	Chapters
Vulnerability and Attack Labs (Linux-based)	Buffer Overflow Vulnerability	1	10
	Return-to-libc Attack	1	10
	Format String Vulnerability	1	10
	Race Condition Vulnerability	1	10
	Set-UID Program Vulnerability	1	7
	Chroot Sandbox Vulnerability	1	-
	Cross-Site Request Forgery Attack	1	18
	Cross-Site Scripting Attack	1	18
	SQL Injection Attack	1	10, 18
	ClickJacking Attack	1	18
	TCP/IP Attacks	2	17
	DNS Pharming Attacks	2	17
Exploration Labs (Linux-based)	Pack Sniffing & Spoofing	1	17
	Pluggable Authentication Module	1	4, 7
	Web Access Control	1	18
	SYN Cookie	1	17
	Linux Capability	1	5
	Secret-Key Encryption	1	14
	One-Way Hash Function	1	14
	Public-Key Infrastructure	1	15
Design and Implementation Labs	Virtual Private Network (Linux)	4	16
	IPSec (Minix)	4	16
	Firewall (Linux)	2	17
	Firewall (Minix)	2	17
	Role-Based Access Control (Minix)	4	5
	Capability-Based Access Control (Minix)	3	5
	Encrypted File System (Minix)	4	14
	Address Space Randomization (Minix)	2	-
	Set-RandomUID Sandbox (Minix)	1	-

Mapping SEED Labs to Textbook Chapters

Security in Computing, 4th Edition
 Charles P. Pfleeger & Shari Lawrence Pfleeger
 Prentice Hall, 2006



Types	Labs	Time (week)	Chapters
Vulnerability and Attack Labs (Linux-based)	Buffer Overflow Vulnerability	1	3
	Return-to-libc Attack	1	3
	Format String Vulnerability	1	3
	Race Condition Vulnerability	1	3
	Set-UID Program Vulnerability	1	4
	Chroot Sandbox Vulnerability	1	3
	Cross-Site Request Forgery Attack	1	3
	Cross-Site Scripting Attack	1	3
	SQL Injection Attack	1	3, 6
	ClickJacking Attack	1	3
	TCP/IP Attacks	2	7
	DNS Pharming Attacks	2	7
Exploration Labs (Linux-based)	Pack Sniffing & Spoofing	1	7
	Pluggable Authentication Module	1	4
	Web Access Control	1	4, 7
	SYN Cookie	1	2, 7
	Linux Capability	1	4
	Secret-Key Encryption	1	2, 12
	One-Way Hash Function	1	2, 12
	Public-Key Infrastructure	1	2, 12
Design and Implementation Labs	Virtual Private Network (Linux)	4	2, 7
	IPSec (Minix)	4	2, 7
	Firewall (Linux)	2	7
	Firewall (Minix)	2	7
	Role-Based Access Control (Minix)	4	4
	Capability-Based Access Control (Minix)	3	4
	Encrypted File System (Minix)	4	2, 4
	Address Space Randomization (Minix)	2	4, 5
	Set-RandomUID Sandbox (Minix)	1	4

Mapping SEED Labs to Textbook Chapters

Introduction to Computer Security
 Matt Bishop
 Addison-Wesley, 2004



Types	Labs	Time (week)	Chapters
Vulnerability and Attack Labs (Linux-based)	Buffer Overflow Vulnerability	1	20, 26
	Return-to-libc Attack	1	20, 26
	Format String Vulnerability	1	20, 26
	Race Condition Vulnerability	1	20, 26
	Set-UID Program Vulnerability	1	14
	Chroot Sandbox Vulnerability	1	20, 26
	Cross-Site Request Forgery Attack	1	20, 23, 26
	Cross-Site Scripting Attack	1	20, 23, 26
	SQL Injection Attack	1	20, 23, 26
	ClickJacking Attack	1	20, 23, 26
	TCP/IP Attacks	2	20, 23, 26
	DNS Pharming Attacks	2	20, 23, 26
Exploration Labs (Linux-based)	Pack Sniffing & Spoofing	1	23
	Pluggable Authentication Module	1	11
	Web Access Control	1	4, 14
	SYN Cookie	1	23
	Linux Capability	1	12, 14, 17
	Secret-Key Encryption	1	8-10
	One-Way Hash Function	1	8-10
	Public-Key Infrastructure	1	8-10
Design and Implementation Labs	Virtual Private Network (Linux)	4	8-10, 17, 23
	IPSec (Minix)	4	8-10, 17, 23
	Firewall (Linux)	2	17, 23
	Firewall (Minix)	2	17, 23
	Role-Based Access Control (Minix)	4	12, 14, 17
	Capability-Based Access Control (Minix)	3	12, 14, 17
	Encrypted File System (Minix)	4	8-10, 17
	Address Space Randomization (Minix)	2	22, 24, 26
	Set-RandomUID Sandbox (Minix)	1	19

Mapping SEED Labs to Textbook Chapters

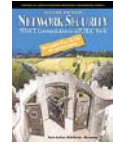
Computer Security: Art and Science
 Matt Bishop
 Addison-Wesley, 2002



Types	Labs	Time (week)	Chapters
Vulnerability and Attack Labs (Linux-based)	Buffer Overflow Vulnerability	1	23, 29
	Return-to-libc Attack	1	23, 29
	Format String Vulnerability	1	23, 29
	Race Condition Vulnerability	1	23, 29
	Set-UID Program Vulnerability	1	15
	Chroot Sandbox Vulnerability	1	23, 29
	Cross-Site Request Forgery Attack	1	23, 26, 29
	Cross-Site Scripting Attack	1	23, 26, 29
	SQL Injection Attack	1	23, 26, 29
	ClickJacking Attack	1	23, 26, 29
	TCP/IP Attacks	2	23, 26, 29
	DNS Pharming Attacks	2	23, 26, 29
Exploration Labs (Linux-based)	Pack Sniffing & Spoofing	1	26
	Pluggable Authentication Module	1	12
	Web Access Control	1	4, 15
	SYN Cookie	1	26
	Linux Capability	1	13, 15, 19
	Secret-Key Encryption	1	9, 10, 11
	One-Way Hash Function	1	9, 10, 11
	Public-Key Infrastructure	1	9, 10, 11
Design and Implementation Labs	Virtual Private Network (Linux)	4	9-11, 19, 26
	IPSec (Minix)	4	9-11, 19, 26
	Firewall (Linux)	2	19, 26
	Firewall (Minix)	2	19, 26
	Role-Based Access Control (Minix)	4	13, 15, 19
	Capability-Based Access Control (Minix)	3	13, 15, 19
	Encrypted File System (Minix)	4	9-11, 13, 19
	Address Space Randomization (Minix)	2	25, 27, 29
	Set-RandomUID Sandbox (Minix)	1	22

Mapping SEED Labs to Textbook Chapters

Network Security: Private Communication in a Public World, 2nd ed.
 Charlie Kaufman, Radia Perlman, & Mike Speciner
 Prentice Hall, 2002



Types	Labs	Time (week)	Chapters
Vulnerability and Attack Labs (Linux-based)	Buffer Overflow Vulnerability	1	-
	Return-to-libc Attack	1	-
	Format String Vulnerability	1	-
	Race Condition Vulnerability	1	-
	Set-UID Program Vulnerability	1	-
	Chroot Sandbox Vulnerability	1	-
	Cross-Site Request Forgery Attack	1	25
	Cross-Site Scripting Attack	1	25
	SQL Injection Attack	1	-
	Clickjacking Attack	1	25
	TCP/IP Attacks	2	-
	DNS Pharming Attacks	2	-
Exploration Labs (Linux-based)	Pack Sniffing & Spoofing	1	5
	Pluggable Authentication Module	1	9, 10
	Web Access Control	1	25
	SYN Cookie	1	5
	Linux Capability	1	-
	Secret-Key Encryption	1	2-6
	One-Way Hash Function	1	2-6
	Public-Key Infrastructure	1	2-6
Design and Implementation Labs	Virtual Private Network (Linux)	4	2-5, 17
	IPSec (Minix)	4	2-5, 17
	Firewall (Linux)	2	23
	Firewall (Minix)	2	23
	Role-Based Access Control (Minix)	4	-
	Capability-Based Access Control (Minix)	3	-
	Encrypted File System (Minix)	4	2-5
	Address Space Randomization (Minix)	2	-
	Set-RandomUID Sandbox (Minix)	1	-