

# Intermediate Security Concepts: UNIX and Linux

Introduction.....	1
Exercise 1: Is This Class Right For You?.....	2
Computer Systems, Usernames, Passwords, and Addresses .....	6
Step 1: Securing the Unix Computer Through Software .....	7
Supervisory Rights.....	7
Controlling Services.....	11
The R-Commands .....	15
Set UID and Set GID .....	15
Other Security Settings .....	16
Exercise 2.....	20
Step 2: Network Sniffers.....	22
Using nmap .....	24
Port Scanners and Probes.....	26
Exercise 3: Setting up a Network Sniffer and Port Scanner .....	27
Step 3: Setting up a Linux Firewall .....	30
Setting up Standard Firewall Rules.....	31
Examples.....	33
Exercise 4: Setting up a Linux Firewall.....	36
Step 4: Intrusion Detection Systems .....	41
Exercise 5: Using Intrusion Detection Server Snort.....	42
Step 5: Public and Private Key Encryption: Pretty Good Privacy (PGP).....	44
General Encryption .....	44
Public and Private Key Encryption.....	47
Electronic Signatures .....	47
Exercise 6: PGP .....	50
Step 6: Secure Communication: Configuring SSH Client/Server .....	55
Installing Server Keys.....	55
Installing User Keys.....	56
Exercise 7: Configuring SSH Client/Server .....	58
Step 7: Detecting Abuses: Tripwire.....	60
Exercise 8: Tripwire.....	71
What To Do If You've Been Compromised.....	73
Appendix A: Network Diagram.....	75