

Course Description: This course provides an introduction to installing, configuring, and maintaining Linux systems from a security perspective. It serves as an administrative guide to implementing security and security tools on Linux. This course will not teach you how to break into systems, although some obvious tricks are described to heighten your awareness. And provide a framework - a foundation if you will - that will allow you to learn more and be as dynamic as the field of computer security itself.

Who Should Attend: Linux/Unix System administrators who want to ensure the integrity and security of their networks and Linux systems will benefit from this course.

Prerequisites: Attendees must have basic knowledge of Unix/Linux commands. System Administrative experience is a plus.

Benefits of Attendance: Upon completion of this course, students will be able to:

- Identify how intrusions happen
- Secure the physical hardware
- Secure the operating system and networks from intrusions
- Maintain and monitor secured systems and networks

Course Outline:

OVERVIEW

Why we need security
Is it really secure?
Technical, Social and Physical Attacks
Identifying a Security Policy
What are you protecting?
Integrity
Hardware Integrity
Restricting the Boot Process
BIOS
Password Protecting LILO
Boot Loader
Password Protecting the GRUB Boot Loader
Single user mode
Security of local devices
Software and data integrity
Search Engines
Domain Registrars
Regional Internet Registries
DNS Reverse-Lookups
Mail Exchange
Zone Transfers
ping and ping Sweeping
Port Scanning
Fingerprinting
traceroute
Establish Sound Password Policies
Control the Root Password
Monitor Non-console Root Logins
Eliminate Generic Accounts
Manage Access Information Availability
Secure Network Services
Detecting Physical Security Compromises

UNDERSTANDING DISCRETIONARY

ACCESS CONTROL

What is SELinux?
NSA SELinux future direction
File System Concepts
File System Structure
Filesystem Types
File Types
Login process
Access startup files
Trusted hosts and user access control
rlogin
rexec
finger
Remote Host Printing
Linux Permissions
User Account Controls
File Permission Applications
Change file permissions
Special Privilege Access
umask
cron
at and batch tools
Audit, syslog

Getting to Know the Shell
The standard input/output (I/O) file
Redirection of standard input and output files
Appending the standard output file
Pipes Appending the standard output file
The standard error file
Quoting mechanisms
The shell prompt variables
File name generation characters
Aliases
Functions
History
Editing the command line
Discretionary Access Control Lab

INSTALLATION AND CONFIGURATION

Partitions & Filesystems
kickstart
Installing Linux
Hardware Requirement
Software Requirement
Patch Control
RedHat Package Manager (RPM)
Using RPM
Installing, upgrading Package
Querying Packages
The X Window System
Installing XFree86
Configuring Xfree86
X Fonts
The X Font Server
The .Xresources file
The X Display Manager
Customizing xdm
Customizing GDM
Customizing Window Manager Environment
xvidtune

DEFINING NETWORK SERVICES

Introduction
Future is more secure with IPv6
IP Addresses
TCP/IP Protocol Family
The TCP/IP Model Layers
Remote Procedure Call (RPC)
Ports
Trusted hosts & related commands
ftp
telnet
Domain Name System (DNS)
NIS
DHCP
DHCP Client
Electronic Mail
sendmail
SNMPD
X Windows & remote X Clients
UUCP

System Logging Daemon (syslogd)
The /etc/syslog.conf File
SSL, S-HTTP and S/MIME
PCNFs
Samba
Defining network services Labs
X Windows & remote X Clients

PASSWORD SECURITY AND

ENCRYPTION

Stronger Passwords
Cryptography
PGP
Installation of PGP
Basic Configuration
Creating the Pair of Keys
Adding keys to a Ring
Removing Keys from a Ring
Extracting a Key
Content of a Ring
Encoding a Message
Encoding a Message for Several Recipients
How to Sign a Message
Decoding
Dealing with Text Files
Using PGP in Shells
ssh (Secure Shell) and stelnets
PAM - Pluggable Authentication Modules
Linux IPSEC Implementations
Using ipsec_tunnel with FreeS/WAN
Using ipsec_tunnel with WatchGuard
Firebox System 5.0
Cryptographic IP Encapsulation (CIPE)
Kerberos

UNIX AND NETWORK SECURITY TOOLS

Sniffers and scanners
Dig
nmap - scanner
crack - remote hacking
SATAN - scanning tool
showmount, war-dialing
ARP redirect
traceroute, tcpdump
ping - scanner
System Services and tcp_wrappers
Sendmail Wrapper Program
Firewalls
Virtual Private Network (VPN)
Network Filesystem (NFS)
Denial of Service Attacks
Tripwire
Intruder Alert (ITA)
ifstatus and cmp

SYSTEM ADMINISTRATION

System Runlevels and /etc/rc*
The /etc/inittab File, ifconfig, route, netstat,
whois, host

sudo, /etc/sudoers
Securing Portmap
Utilizing system logs
System Administration labs