

**Course Description:** This course will help Linux and UNIX Systems Administrators in making their systems and networks as secure as possible from intruders and improper action of the users. It covers both quick and simple solutions, and some more involved solutions to eliminate possible vulnerability.

**Who Should Attend:** Everyone

**Prerequisites:** Students should have Linux Systems Administration experience. Basic Network knowledge is a plus.

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

- Understand hacking techniques and countermeasures
- Solve common security problems
- Understand and prevent wireless hacking
- Setup Security Policy
- Understand and implement access control
- Determine who to trust and when to trust
- Understand Firewall vulnerabilities and implement countermeasures
- Utilize VPN (Virtual Private Networks) for secure connections
- understand Host Hardening techniques
- Secure subsystems
- Scan systems
- Find and repair damage

### Course Outline:

#### Introduction

Introduction  
 What Are You Trying To Protect?  
 In the Beginning  
 Somebody@Somewhere  
 The Underlying Problem in Today's TCP/IP  
 The TCP/IP Model Layers  
 Future is More Secure With IPv6  
 IPSec  
 Who Are the Enemies and What Do They Want?  
 Type of Attacks  
 Technical Attacks  
 Social Attacks  
 Physical Attacks  
 Wireless Attacks  
 Most Common Mistakes  
 Weak Passwords  
 Open Network Ports  
 Outdated Software  
 Badly Configured and Insecure Programs  
 Obsolete or Benign Accounts  
 I'll Do It Tomorrow  
 Viruses and Linux  
 Detecting an Intrusion and Preventing Further Attacks  
 Tripwire

#### Understanding the Hacking Techniques

Understanding Hacking Techniques  
 Footprinting  
 Search Engines  
 Domain Registrars  
 Regional Internet Registries  
 DNS Reverse-Lookups  
 Mail Exchange  
 Zone Transfers  
 Traceroute  
 Scanning and Identification  
 Ping and Ping Sweeping  
 TCP Pinging  
 Port Scanning  
 Fingerprinting  
 Remote Hacking  
 Ports at Risk

#### Technical Attacks Explained

Technical Attacks Explained  
 Attack Paths  
 Rootkit Attacks  
 Packet Spoofing  
 SYN Flood Attack  
 TCP Sequence Spoofing  
 Packet Storms, Smurf Attacks, and Fraggles  
 Buffer Overflows or Stamping on Memory With gets()  
 Man-in-the-Middle Attack  
 Wireless Attacks Explained

Wireless Standards  
 WEP, WPA, and WPA 2  
 Probing & Network Discovery  
 Surveillance  
 DOS Attacks  
 Impersonation  
 Man in the Middle and Rouge AP

#### Access Control

Introduction  
 The Highest Security  
 Access Control  
 Identification and Authentication  
 Access Control Types  
 Access Control Models  
 SSL Certificates  
 Authenticating with PAM  
 Password Management  
 Hardware Password Protection  
 Password Protecting the GRUB Boot Loader  
 Advanced Password Methods  
 Different Functions of Different Algorithms  
 MD5 Passwords  
 Password Aging  
 Use `sudo` to Protect Root Access  
 File Protection  
 The `chattr` Program and the Immutable Bit  
 Cryptography  
 Protect Files With GPG  
 Using Encrypted Keys  
 Default Setting For Single User Mode  
 Login Simulators  
 Warning Banners  
 Add Security to `/bin/login`  
 User Startup Files  
 Useful Tools  
 Account Controls  
 Restrict `at` and `cron` Access  
 More Default Settings  
 Protocol Switches in The Kernel  
 Logging Environment

#### Security Policy

Setup Security Policy  
 Standards and Regulations  
 Why Your Organization Needs Security Policies  
 Security Policy Basics  
 Administrative Policies vs. Technical Policies  
 Administrative Security Policy Samples  
 Technical Security Policy Samples

#### Network Access Security

Network Access Security  
 Ring Security  
 Modem Access  
 X Security

TCP-wrappers  
 Virtual Private Networks (VPN)  
 Protecting Network Connections - SSH2  
 Install and Configure SSH  
 Restricting Host Access - SSH Server  
 SSH Authentication  
 OpenSSH Client and OpenSSH Server  
 Authenticate Between an SSH2 Client and an OpenSSH Server  
 Tunneling with SSH  
 Ports at Risk  
`ifconfig`  
`xinetd` and `inetd`  
 Adding New Services `xinetd` `inetd`  
 Restricting Remote User Access  
 Restricting Remote Host Access `xinetd`  
 Restricting Remote Host Access - `xinetd` with `libwrap`  
 Defending Against Denial of Service (DoS) Attacks  
 Harden `inetd` and `xinetd` Configurations  
 Firewalls  
 Firewalls with `iptables`, `ipchains` and `DMZ`  
 Tunneling Through Firewalls  
 Egress Filtering

#### Host Hardening

Host Hardening  
 SELinux - NSA Security-Enhanced Linux (SELinux)  
 AppArmor  
 LDAP  
 Postfix  
 Qpopper  
`sendmail`  
 BIND (DNS)  
 Apache  
 Samba  
 NFS

#### Scanning Your Own System

Scanning Your Own System  
 Top 20 Security Tools  
 The Nessus Security Scanner  
 Wireshark (Ethereal)  
 Snort Attack Detector  
`netcat`  
 John the Ripper  
 Crack  
 Store the RPM Database Checksums  
 Finding and Repairing the Damage  
 Information Systems' Security Response to Intrusions  
 The IT Response to Intrusions  
 The Law Enforcement Response to Intrusions  
 Information to Determine Damages or Loss