GL-275: Red Hat Linux Network Services

Course Length: 5 days

Course Description: The GL275 is an expansive course that covers a wide range of network services useful to every organization. Special attention is paid to the concepts needed to implement these services securely, and to the trouble-shooting skills which will be necessary for real-world administration of these network services. Like all Guru Labs courses, the course material is designed to provide extensive hands-on experience. Topics include: Security with SELinux and Netfilter, DNS concepts and implementation with Bind; LDAP concepts and implementation using OpenLDAP; Web services with Apache; FTP with vsftpd; caching, filtering proxies with Squid; SMB/CIFS (Windows networking) with Samba; and e-mail concepts and implementation with Postfix combined with either Dovecot or Cyrus.

Prerequisites: Students should already be comfortable with basic Linux or Unix administration. Fundamentals such as the Linux filesystem, process management, and how to edit files will not be covered in class. A good understanding of network concepts, the TCP/IP protocol suite is also assumed. These skills are taught in the GL120 "Linux Fundamentals" and GL250 "Enterprise Linux Systems Administration" courses.

Distributions: Red Hat Enterprise Linux 8

Course Outline

1 **SECURING SERVICES**
   1 Xinetd
   2 Xinetd Connection Limiting and Access Control
   3 Xinetd: Resource limits, redirection, logging
   4 TCP Wrappers
   5 The /etc/hosts.allow & /etc/hosts.deny Files
   6 /etc/hosts.{allow,deny} Shortcuts
   7 Advanced TCP Wrappers
   8 FirewallD
   9 Netfilter: Stateful Packet Filter Firewall
   10 Netfilter Concepts
   11 Using the iptables Command
   12 Netfilter Rule Syntax
   13 Targets
   14 Common match_specs
   15 Connection Tracking

   LAB TASKS
   1 Securing xinetd Services
   2 Enforcing Security Policy with xinetd
   3 Securing Services with TCP Wrappers
   4 Securing Services with Netfilter
   5 FirewallD
   6 Troubleshooting Practice

2 **SELINUX AND LSM**
   1 SELinux Security Framework
   2 Choosing an SELinux Policy
   3 SELinux Commands
   4 SELinux Booleans
   5 SELinux Policy Tools

   LAB TASKS
   1 SELinux File Contexts

3 **DNS CONCEPTS**