

Course Length: 5 days

This class focuses on network security, and makes an excellent companion class to the GL550: Enterprise Linux Security Administration course. After a detailed discussion of the TCP/IP suite component protocols and ethernet operation, the student practices using various tools to capture, analyze, and generate IP traffic. Students then explore the tools and techniques used to exploit protocol weaknesses and perform more advanced network attacks. After building a thorough understanding of network based attacks, course focus shifts to the defensive solutions available. Students install, configure, and test two of the most popular and powerful NIDS solutions available. Finally, students create a Linux based router / firewall solution, including advanced functionality such as NAT, policy routing, and traffic shaping.

Prerequisites:

Since the tools used in class are compiled and run on a Linux system, Linux or UNIX system experience is helpful, but not necessary. A solid background in networking concepts will greatly aid in comprehension. This is an intense class that covers many topics. If you are unsure if you meet the prerequisites, please speak with a [Guru Labs' representative](#).

Supported Distributions: Red Hat Enterprise Linux 3

Course Outline:

1. Ethernet and IP Operation
2. IP And ARP Vulnerability Analysis
3. UDP/TCP Protocol and TELNET Vulnerability Analysis
4. FTP And HTTP Vulnerability Analysis
5. DNS Protocol Vulnerability
6. SSH and HTTPS Protocol Vulnerability Analysis
7. Remote Operating System
8. Attacks and Basic Attack Detection
9. Intrusion Detection Technologies
10. Advanced Snort Configuration
11. Snort Rules
12. Linux and Static Routing
13. Linux Firewalls
14. Network and Port Address
15. IP Policy Routing