Red Hat Enterprise Linux – Security

Description: The Red Hat Enterprise Linux Security course covers the knowledge and skills a student will need to effectively secure a RHEL installation. Class begins with a discussion of basic security topics, including firewalls, logging, security concepts, documentation and best practices. Moving forward, the class delves into specific security tools and labs, exploring common attack vectors along with their detection and resolution techniques. As a method of applying learned concepts, the students will work on hardening their machines for specific services, such as DNS servers, web servers, SSH servers, mail servers and more.

Objectives:

Upon successful completion of the course, the student will…

1) Understand basic security concepts, such as authentication, authorization, threat identification/mitigation and access controls
2) Understand how to implement efficient and effective firewalls, including TCP Wrappers and IPTables.
3) Understand various cryptographic models and systems, including PKI, SSL, symmetric/asymmetric encryption and common algorithms.
4) Understand NFSv3 and NFSv4 security best practices.
5) Understand SSH and FTP security considerations and best practices.
6) Understand web server security concerns on the Apache web server, including topics such as server misconfiguration, CGI scripting, permissions and more.
7) Understand intrusion detection methods and tools, including Tripwire, Snort, log analysis and root kits.
8) Understand how to properly deploy secure authentication through Kerberos.
9) Understand the SELinux extensions available in the kernel and how to leverage them to increase system security.

Outline:

1) Security Basic Concepts
    a. Goals and misconceptions
    b. Threat identification
    c. Threat mitigation techniques
    d. Authentication versus authorization
2) Firewalls
    a. TCP Wrappers
    b. IPTables
3) Cryptography
    a. Ciphering, Hashing, basic algorithms
    b. PKI
    c. SSL
4) SELinux
    a. High level overview
    b. Contexts and the AVC
    c. Policy
5) Intrusion detection
    a. Log analysis
    b. Filesystem crumbs
    c. Root kits
    d. Fingerprinting
        d.i. Tripwire, Osiris
    e. Active monitoring with Snort
6) NFS
    a. Version 3
    b. Version 4
7) Kerberos
    a. Basic implementation
    b. Security considerations and configurations
8) Web Servers – Apache
    a. Intentional and unintentional misconfigurations
    b. CGI, PHP concerns