Course duration

- 5 days

Course Benefits

- Learn a broad range of general security techniques such as packet filtering, password policies, and file-integrity checking.
- Learn advanced security technologies such as Kerberos and SELinux.
- Learn to secure commonly deployed network services.
- Gain an excellent understanding of potential security vulnerabilities.
- Learn to audit existing machines and how to securely deploy new network services. .

Course Outline

1. Security Concepts
    1. Basic Security Principles
    2. RHEL7 Default Install
    3. RHEL7 Firewall
    4. SLES12 Default Install
    5. SUSE Basic Firewall Configuration
    6. SLES12: File Security
    7. Minimization – Discovery
    8. Service Discovery
    9. Hardening
    10. Security Concepts
    11. Lab Tasks
        1. Removing Packages Using RPM
        2. Firewall Configuration
        3. Process Discovery
        4. Operation of the setuid() and capset() System Calls
        5. Operation of the chroot() System Call
2. Scanning, Probing, and Mapping Vulnerabilities
    1. The Security Environment
    2. Stealth Reconnaissance
    3. The WHOIS database
    4. Interrogating DNS
    5. Discovering Hosts
    6. Discovering Reachable Services
    7. Reconnaissance with SNMP
    8. Discovery of RPC Services
    9. Enumerating NFS Shares

10. Nessus/OpenVAS Insecurity Scanner
11. Configuring OpenVAS
12. Intrusion Detection Systems
13. Snort Rules
14. Writing Snort Rules
15. Lab Tasks
    1. NMAP
    2. OpenVAS
    3. Advanced nmap Options

3. Password Security and PAM
    1. Unix Passwords
    2. Password Aging
    3. Auditing Passwords
    4. PAM Overview
    5. PAM Module Types
    6. PAM Order of Processing
    7. PAM Control Statements
    8. PAM Modules
    9. pam_unix
    10. pam_cracklib.so
    11. pam_pwcheck.so
    12. pam_env.so
    13. pam_xauth.so
    14. pam_tally2.so
    15. pam_wheel.so
    16. pam_limits.so
    17. pam_nologin.so
    18. pam_deny.so
    19. pam_warn.so
    20. pam_securetty.so
    21. pam_time.so
    22. pam_access.so
    23. pam_listfile.so
    24. pam_lastlog.so
    25. pam_console.so
    26. Lab Tasks
        1. John the Ripper
        2. Cracklib
        3. Using pam_listfile to Implement Arbitrary ACLs
        4. Using pam_limits to Restrict Simultaneous Logins
        5. Using pam_nologin to Restrict Logins
        6. Using pam_access to Restrict Logins
        7. su & pam
4. Secure Network Time Protocol (NTP)
    1. The Importance of Time
    2. Hardware and System Clock
    3. Time Measurements

4. NTP Terms and Definitions
5. Synchronization Methods
6. NTP Evolution
7. Time Server Hierarchy
8. Operational Modes
9. NTP Clients
10. Configuring NTP Clients
11. Configuring NTP Servers
12. Securing NTP
13. NTP Packet Integrity
14. Useful NTP Commands
15. Lab Tasks
    1. Configuring and Securing NTP
    2. Peering NTP with Multiple Systems

5. Kerberos Concepts and Components
    1. Common Security Problems
    2. Account Proliferation
    3. The Kerberos Solution
    4. Kerberos History
    5. Kerberos Implementations
    6. Kerberos Concepts
    7. Kerberos Principals
    8. Kerberos Safeguards
    9. Kerberos Components
    10. Authentication Process
    11. Identification Types
    12. Logging In
    13. Gaining Privileges
    14. Using Privileges
    15. Kerberos Components and the KDC
    16. Kerberized Services Review
    17. KDC Server Daemons
    18. Configuration Files
    19. Utilities Overview
6. Implementing Kerberos
    1. Plan Topology and Implementation
    2. Kerberos 5 Client Software
    3. Kerberos 5 Server Software
    4. Synchronize Clocks
    5. Create Master KDC
    6. Configuring the Master KDC
    7. KDC Logging
    8. Kerberos Realm Defaults
    9. Specifying [realms]
    10. Specifying [domain_realm]
    11. Allow Administrative Access
    12. Create KDC Databases

13. Create Administrators
14. Install Keys for Services
15. Start Services
16. Add Host Principals
17. Add Common Service Principals
18. Configure Slave KDCs
19. Create Principals for Slaves
20. Define Slaves as KDCs
21. Copy Configuration to Slaves
22. Install Principals on Slaves
23. Synchronization of Database
24. Propagate Data to Slaves
25. Create Stash on Slaves
26. Start Slave Daemons
27. Client Configuration
28. Install krb5.conf on Clients
29. Client PAM Configuration
30. Install Client Host Keys
31. Lab Tasks
    1. Implementing Kerberos

7. Administering and Using Kerberos
    1. Administrative Tasks
    2. Key Tables
    3. Managing Keytabs
    4. Managing Principals
    5. Viewing Principals
    6. Adding, Deleting, and Modifying Principals
    7. Principal Policy
    8. Overall Goals for Users
    9. Signing In to Kerberos
    10. Ticket types
    11. Viewing Tickets
    12. Removing Tickets
    13. Passwords
    14. Changing Passwords
    15. Giving Others Access
    16. Using Kerberized Services
    17. Kerberized FTP
    18. Enabling Kerberized Services
    19. OpenSSH and Kerberos
    20. Lab Tasks
        1. Using Kerberized Clients
        2. Forwarding Kerberos Tickets
        3. OpenSSH with Kerberos
        4. Wireshark and Kerberos
8. Securing the Filesystem
    1. Filesystem Mount Options

2. NFS Properties
3. NFS Export Option
4. NFSv4 and GSSAPI Auth
5. Implementing NFSv4
6. Implementing Kerberos with NFS
7. GPG – GNU Privacy Guard
8. File Encryption with OpenSSL
9. File Encryption With encfs
10. Linux Unified Key Setup (LUKS)
11. Lab Tasks
    1. Securing Filesystems
    2. Securing NFS
    3. Implementing NFSv4
    4. File Encryption with GPG
    5. File Encryption With OpenSSL
    6. LUKS-on-disk format Encrypted Filesystem

9. AIDE
    1. Host Intrusion Detection Systems
    2. Using RPM as a HIDS
    3. Introduction to AIDE
    4. AIDE Installation
    5. AIDE Policies
    6. AIDE Usage
    7. Lab Tasks
    8. File Integrity Checking with RPM
    9. File Integrity Checking with AIDE
10. Accountability with Kernel Auditd
    1. Accountability and Auditing
    2. Simple Session Auditing
    3. Simple Process Accounting & Command History
    4. Kernel-Level Auditing
    5. Configuring the Audit Daemon
    6. Controlling Kernel Audit System
    7. Creating Audit Rules
    8. Searching Audit Logs
    9. Generating Audit Log Reports
    10. Audit Log Analysis
    11. Lab Tasks
        1. Auditing Login/Logout
        2. Auditing File Access
        3. Auditing Command Execution
11. SELinux
    1. DAC vs. MAC
    2. Shortcomings of Traditional Unix Security
    3. AppArmor
    4. SELinux Goals
    5. SELinux Evolution

6. SELinux Modes
7. Gathering SELinux Information
8. SELinux Virtual Filesystem
9. SELinux Contexts
10. Managing Contexts
11. The SELinux Policy
12. Choosing an SELinux Policy
13. Policy Layout
14. Tuning and Adapting Policy
15. Booleans
16. Permissive Domains
17. Managing File Context Database
18. Managing Port Contexts
19. SELinux Policy Tools
20. Examining Policy
21. SELinux Troubleshooting
22. SELinux Troubleshooting Continued
23. Lab Tasks
    1. Exploring SELinux Modes
    2. Exploring AppArmor Modes
    3. SELinux Contexts in Action
    4. Exploring AppArmor
    5. Managing SELinux Booleans
    6. Creating Policy with Audit2allow
    7. Creating & Compiling Policy from Source

12. Securing Apache
    1. Apache Overview
    2. httpd.conf – Server Settings
    3. Configuring CGI
    4. Turning Off Unneeded Modules
    5. Delegating Administration
    6. Apache Access Controls (mod_access)
    7. HTTP User Authentication
    8. Standard Auth Modules
    9. HTTP Digest Authentication
    10. TLS Using mod_ssl.so
    11. Authentication via SQL
    12. Authentication via LDAP
    13. Authentication via Kerberos
    14. Scrubbing HTTP Headers
    15. Metering HTTP Bandwidth
    16. Lab Tasks
        1. Hardening Apache by Minimizing Loaded Modules
        2. Scrubbing Apache & PHP Version Headers
        3. Protecting Web Content
        4. Protecting Web Content
        5. Using the suexec Mechanism

6. Create a TLS CA key pair
7. Using SSL CA Certificates with Apache
8. Enable Apache SSL Client Certificate Authentication
9. Enabling SSO in Apache with mod_auth_kerb

13. Securing PostgreSQL
    1. PostgreSQL Overview
    2. PostgreSQL Default Config
    3. Configuring TLS
    4. Client Authentication Basics
    5. Advanced Authentication
    6. Ident-based Authentication
    7. Lab Tasks
        1. Configure PostgreSQL
        2. PostgreSQL with TLS
        3. PostgreSQL with Kerberos Authentication
        4. Securing PostgreSQL with Web Based Applications

Class Materials

Each student will receive a comprehensive set of materials, including course notes and all the class examples.

Class Prerequisites

Experience in the following *is required* for this Linux class:

- Current Linux or UNIX systems administration experience.