Szkolenie: Compendium CE
Enterprise Linux Security Administration

Cel szkolenia:

Ten techniczny kurs skupia się na prawidłowym zabezpieczeniu maszyn z systemem operacyjnym Linux. Obejmuje szeroki zakres ogólnych technik bezpieczeństwa, takich jak filtrowanie pakietów, zasady haseł i sprawdzanie integralności plików. Uczestnicy poznają również zaawansowane technologie bezpieczeństwa, takie jak Kerberos i SELinux. Szczególną uwagę zwraca się na zabezpieczenie powszechnie wdrażanych usług sieciowych. Po zakończeniu kursu studenci będą mieli doskonałe zrozumienie potencjalnych luk w zabezpieczeniach, nauczą się audytować istniejące maszyny oraz bezpiecznie wdrażać nowe usługi sieciowe.

Grupa docelowa

- **Specjaliści ds. cyberbezpieczeństwa:** Analitycy bezpieczeństwa i profesjonaliści, którzy potrzebują zrozumienia administracji systemami, szczególnie w środowisku Linux, aby lepiej zabezpieczać i zarządzać infrastrukturą IT swojej organizacji.

Plan szkolenia:

- SECURITY CONCEPTS
  - Basic Security Principles
  - RHEL7 Default Install
  - RHEL7 Firewall
  - SLES12 Default Install
  - SUSE Basic Firewall Configuration
  - SLES12: File Security
  - Minimization - Discovery
  - Service Discovery
  - Hardening
  - Security Concepts
- SCANNING, PROBING, AND MAPPING VULNERABILITIES
  - The Security Environment
  - Stealth Reconnaissance

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- The WHOIS database
- Interrogating DNS
- Discovering Hosts
- Discovering Reachable Services
- Reconnaissance with SNMP
- Discovery of RPC Services
- Enumerating NFS Shares
- Nessus/OpenVAS Insecurity Scanner
- Configuring OpenVAS
- Intrusion Detection Systems
- Snort Rules
- Writing Snort Rules

- PASSWORD SECURITY AND PAM
  - Unix Passwords
  - Password Aging
  - Auditing Passwords
  - PAM Overview
  - PAM Module Types
  - PAM Order of Processing
  - PAM Control Statements
  - PAM Modules
  - pam_unix
  - so
- SECURE NETWORK TIME PROTOCOL (NTP)
  - The Importance of Time
  - Hardware and System Clock
  - Time Measurements
  - NTP Terms and Definitions
  - Synchronization Methods
  - NTP Evolution
  - Time Server Hierarchy
  - Operational Modes
  - NTP Clients
  - Configuring NTP Clients
  - Configuring NTP Servers
  - Securing NTP

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- NTP Packet Integrity
- Useful NTP Commands

- KERBEROS CONCEPTS AND COMPONENTS
  - Common Security Problems
  - Account Proliferation
  - The Kerberos Solution
  - Kerberos History
  - Kerberos Implementations
  - Kerberos Concepts
  - Kerberos Principals
  - Kerberos Safeguards
  - Kerberos Components
  - Authentication Process
  - Identification Types
  - Logging In
  - Gaining Privileges
  - Using Privileges
  - Kerberos Components and the KDC
  - Kerberized Services Review
  - KDC Server Daemons
  - Configuration Files
  - Utilities Overview
- IMPLEMENTING KERBEROS
  - Plan Topology and Implementation
  - Kerberos 5 Client Software
  - Kerberos 5 Server Software
  - Synchronize Clocks
  - Create Master KDC
  - Configuring the Master KDC
  - KDC Logging
  - Kerberos Realm Defaults
  - Specifying [realms]
  - Specifying [domain_realm]
  - Allow Administrative Access
  - Create KDC Databases
  - Create Administrators

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Install Keys for Services
- Start Services
- Add Host Principals
- Add Common Service Principals
- Configure Slave KDCs
- Create Principals for Slaves
- Define Slaves as KDCs
- Copy Configuration to Slaves
- Install Principals on Slaves
- Synchronization of Database
- Propagate Data to Slaves
- Create Stash on Slaves
- Start Slave Daemons
- Client Configuration
- Install krb5.conf on Clients
- Client PAM Configuration
- Install Client Host Keys

- ADMINISTERING AND USING KERBEROS
  - Administrative Tasks
  - Key Tables
  - Managing Keytabs
  - Managing Principals
  - Viewing Principals
  - Adding, Deleting, and Modifying Principals
  - Principal Policy
  - Overall Goals for Users
  - Signing In to Kerberos
  - Ticket types
  - Viewing Tickets
  - Removing Tickets
  - Passwords
  - Changing Passwords
  - Giving Others Access
  - Using Kerberized Services
  - Kerberized FTP
  - Enabling Kerberized Services

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- OpenSSH and Kerberos
- SECURING THE FILESYSTEM
  - Filesystem Mount Options
  - NFS Properties
  - NFS Export Option
  - NFSv4 and GSSAPI Auth
  - Implementing NFSv4
  - Implementing Kerberos with NFS
  - GPG – GNU Privacy Guard
  - File Encryption with OpenSSL
  - File Encryption With encfs
  - Linux Unified Key Setup (LUKS)
- AIDE
  - Host Intrusion Detection Systems
  - Using RPM as a HIDS
  - Introduction to AIDE
  - AIDE Installation
  - AIDE Policies
  - AIDE Usage
- ACCOUNTABILITY WITH KERNEL AUDITD
  - Accountability and Auditing
  - Simple Session Auditing
  - Simple Process Accounting & Command History
  - Kernel-Level Auditing
  - Configuring the Audit Daemon
  - Controlling Kernel Audit System
  - Creating Audit Rules
  - Searching Audit Logs
  - Generating Audit Log Reports
  - Audit Log Analysis
- SELINUX
  - DAC vs. MAC
  - Shortcomings of Traditional Unix Security
  - AppArmor
  - SELinux Goals
  - SELinux Evolution

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- SELinux Modes
- Gathering SELinux Information
- SELinux Virtual Filesystem
- SELinux Contexts
- Managing Contexts
- The SELinux Policy
- Choosing an SELinux Policy
- Policy Layout
- Tuning and Adapting Policy
- Booleans
- Permissive Domains
- Managing File Context Database
- Managing Port Contexts
- SELinux Policy Tools
- Examining Policy
- SELinux Troubleshooting
- SELinux Troubleshooting Continued

- SECURING APACHE
  - Apache Overview
  - conf - Server Settings
  - Configuring CGI
  - Turning Off Unneeded Modules
  - Delegating Administration
  - Apache Access Controls (mod_access)
  - HTTP User Authentication
  - Standard Auth Modules
  - HTTP Digest Authentication
  - TLS Using mod_ssl.so
  - Authentication via SQL
  - Authentication via LDAP
  - Authentication via Kerberos
  - Scrubbing HTTP Headers
  - Metering HTTP Bandwidth
- SECURING POSTGRESQL
  - PostgreSQL Overview
  - PostgreSQL Default Config

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Configuring TLS
- Client Authentication Basics
- Advanced Authentication
- Ident-based Authentication

- SECURING EMAIL SYSTEMS
  - SMTP Implementations
  - Security Considerations
  - chrooting Postfix
  - Email with GSSAPI/Kerberos Auth

Wymagania:

Ten kurs obejmuje zaawansowane tematy bezpieczeństwa i jest przeznaczony dla doświadczonych administratorów systemów. Uczestnicy powinni posiadać aktualne doświadczenie w administracji systemami Linux lub UNIX, równoważne kursom **Linux Fundamentals**, **Enterprise Linux Systems Administration** oraz **Enterprise Linux Network Services**

Poziom trudności

Certyfikaty:

Każdy uczestnik otrzymuje zaświadczenie o ukończeniu szkolenia wystawiony przez Compendium CE.

Prowadzący:

Trener Compendium CE posiadający akredytację trenerską wiodących producentów (m.in. SUSE i The Linux Foundation)

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001