

Tytuł szkolenia: Enterprise Linux Network Services (GL275)

Kod szkolenia: H7092S

Wprowadzenie

This is an expansive course covering a wide range of network services. Attention is paid to the concepts needed to implement and troubleshoot the network services securely and 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 email concepts and implementation with Postfix combined with either Dovecot or Cyrus.

Adresaci szkolenia

- New Linux system administrators

Prerequisites

- UNIX® Fundamentals (51434S) or
- Linux Fundamentals (U8583S) and
- Enterprise Linux Systems Administration (H7091S)

Cel szkolenia

At the conclusion of this course, you should be able to:

- Gain the knowledge and skills required to setup, configure, and manage the most popular network services available for Red Hat and SUSE Linux systems

Benefits to you:

- Effectively use networking services and security options
- Understand and configure services to your specific needs
- Avoid unwanted emails by configuring mail services with spam filtering

Czas i forma szkolenia

- 35 godzin (5 dni x 7 godzin), w tym wykłady i warsztaty praktyczne.

Plan szkolenia

Module 1: Securing services

- Xinetd
- Xinetd Connection limiting and access control
- Xinetd: Resource limits, redirection, logging
- TCP wrappers
- The /etc/hosts.allow and /etc/hosts.deny files
- /etc/hosts.{allow,deny} shortcuts
- Advanced TCP wrappers
- SUSE basic firewall configuration
- FirewallD
- Netfilter: Stateful packet filter firewall
- Netfilter Concepts

- Using the iptables command
- Netfilter rule syntax
- Targets
- Common match_specs
- Connection tracking

Lab Tasks

- Securing xinetd Services
- Enforcing Security Policy with xinetd
- Securing Services with TCP Wrappers
- Securing Services with SUSEfirewall2
- Securing Services with Netfilter
- FirewallD
- Troubleshooting Practice

Module 2: SELinux and LSM

- AppArmor
- SELinux security framework
- Choosing an SELinux policy
- SELinux commands
- SELinux Booleans
- SELinux policy tools

Lab Tasks

- Exploring AppArmor Modes
- SELinux File Contexts

Module 3: DNS concepts

- Naming Services
- DNS - A better way
- The domain name space
- Delegation and zones
- Server roles
- Resolving names
- Resolving IP addresses
- Basic BIND administration
- Configuring the resolver
- Testing resolution Lab Tasks
- Configuring a Slave Name Server

Module 4: Configuring BIND

- BIND configuration files
- named.conf Syntax
- named.conf options block
- Creating a site-wide cache
- rndc key configuration
- Zones in named.conf
- Zone database file Syntax
- SOA - start of authority
- A, AAAA, and PTR - Address and pointer records
- NS - Name Server
- TXT, CNAME, and MX - text, alias, and mail host
- SRV - SRV service records
- Abbreviations and gotchas
- \$GENERATE, \$ORIGIN, and \$INCLUDE

Lab Tasks

- Use rndc to Control named
- Configuring BIND Zone Files

Module 5: Creating DNS Hierarchies

- Subdomains and delegation
- Subdomains
- Delegating zones
- in-addr.arpa. delegation
- Issues with in-addr.arpa.
- RFC2317 and in-addr.arpa.

Lab Tasks

- Create a Subdomain in an Existing Domain
- Subdomain Delegation

Module 6: Advanced BIND DNS features

- Address Match Lists and ACLs
- Split namespace with views
- Restricting Queries
- Restricting zone transfers
- Running BIND in a chroot
- Dynamic DNS concepts
- Allowing dynamic DNS updates
- DDNS administration with nsupdate
- Common problems
- Securing DNS with TSIG

Lab Tasks

- Configuring Dynamic DNS
- Securing BIND DNS

Module 7: Using Apache

- HTTP operation
- Apache architecture
- Dynamic shared objects
- Adding modules to Apache
- Apache configuration files
- httpd.conf-Server settings
- httpd.conf-Main configuration
- HTTP Virtual servers
- Virtual hosting DNS implications
- httpd.conf-VirtualHost configuration
- Port and IP based virtual hosts
- Name-based virtual host
- Apache logging
- Log analysis
- The webalizer

Lab Tasks

- Apache Architecture
- Apache Content
- Configuring Virtual Hosts

Module 8: Apache security

- Virtual hosting security implications
- Delegating administration
- Directory protection
- Directory protection with AllowOverride
- Common uses for .htaccess

- Symmetric encryption algorithms
- Asymmetric encryption algorithms
- Digital certificates
- TLS using mod_ssl.so

Lab Tasks

- Using .htaccess Files
- Using TLS Certificates with Apache
- Use SNI and TLS with Virtual Hosts

Module 9: Apache server - side scripting administration

- Dynamic HTTP content
- PHP: Hypertext preprocessor
- Developer tools for PHP
- Installing PHP
- Configuring PHP
- Securing PHP
- Security related php.ini configuration
- Java servlets and JSP
- Apache's Tomcat
- Installing Java SDK
- Installing Tomcat manually
- Using Tomcat with Apache

Lab Tasks

- CGI Scripts in Apache
- Apache's Tomcat
- Using Tomcat with Apache
- Installing Applications with Apache and Tomcat

Module 10: Implementing an FTP server

- The FTP protocol
- Active mode FTP
- Passive mode FTP
- ProFTPD
- Pure-FTPd
- vsftpd
- Configuring vsftpd
- Anonymous FTP with vsftpd

Lab Tasks

- Configuring vsftpd

Module 11: The Squid Proxy server

- Squid overview
- Squid file layout
- Squid access control lists
- Applying Squid ACLs
- Tuning Squid and configuring cache Hierarchies
- Bandwidth metering
- Monitoring Squid
- Proxy client configuration

Lab Tasks

- Installing and Configuring Squid
- Squid Cache Manager CGI
- Proxy Auto Configuration
- Configure a Squid Proxy Cluster

Module 12: SQL fundamentals and MariaDB

- Popular SQL databases
- SELECT statements
- INSERT statements
- UPDATE statements
- DELETE statements
- JOIN clauses
- MariaDB
- MariaDB installation and security
- MariaDB user account management
- MariaDB replication

Lab Tasks

- SQL with SQLite3
- Installing and Securing MariaDB
- Creating a database in MariaDB
- Create a database backed application

Module 13: LDAP concepts and clients

- LDAP: History and uses
- LDAP: Data model basics
- LDAP: Protocol basics
- LDAP: Applications
- LDAP: Search filters
- LDIF: LDAP data interchange format
- OpenLDAP Client Tools
- Alternative LDAP tools

Lab Tasks

- Querying LDAP

Module 14: OpenLDAP servers

- Popular LDAP server implementations
- OpenLDAP: Server architecture
- OpenLDAP: Backends
- OpenLDAP: Replication
- Managing slapd
- OpenLDAP: Configuration options
- OpenLDAP: Configuration sections
- OpenLDAP: Global parameters
- OpenLDAP: Database parameters
- OpenLDAP: Server tools
- Native LDAP authentication and migration
- Enabling LDAP-based login
- System Security Services Daemon (SSSD)

Lab Tasks

- Building An OpenLDAP Server
- Enabling TLS For An OpenLDAP Server
- Enabling LDAP-based Logins

Module 15: Samba concepts and configuration

- Introducing Samba
- NetBIOS and NetBEUI
- Samba Daemons
- Accessing Windows/Samba shares from Linux
- Samba utilities
- Samba configuration files

- The smb.conf file
- Mapping permissions and ACLs
- Mapping Linux concepts
- Mapping users
- Sharing home directories
- Sharing printers
- Share authentication
- Share-level access
- User-level access
- Samba account database
- User share restrictions

Lab Tasks

- Samba Share-Level Access
- Samba User-Level Access
- Samba Group Shares
- Handling Symbolic Links with Samba
- Samba Home Directory Shares

Module 16: SMTP theory

- SMTP
- SMTP terminology
- SMTP architecture
- SMTP commands
- SMTP extensions
- SMTP AUTH
- SMTP STARTTLS
- SMTP session

Module 17: Postfix

- Postfix features
- Postfix architecture
- Postfix components
- Postfix configuration
- master.cf
- main.cf
- Postfix map types
- Postfix pattern matching
- Advanced Postfix options
- Virtual domains
- Postfix mail filtering
- Configuration commands
- Management commands
- Postfix logging
- Logfile analysis
- Postfix, relaying and SMTP AUTH
- SMTP AUTH server and Relay control
- SMTP AUTH clients
- Postfix/TLS
- TLS server configuration
- Postfix client configuration for TLS
- Other TLS clients
- Ensuring TLS security

Lab Tasks

- Configuring Postfix
- Postfix Virtual Host Configuration
- Postfix Network Configuration
- Postfix SMTP AUTH Configuration
- Postfix STARTTLS Configuration
- SUSE Postfix Configuration Cleanup

Module 18: Mail Services and Retrieval

- Filtering Email
- Procmal
- SpamAssassin
- Bogofilter
- amavisd-new Mail Filtering
- Accessing Email
- The IMAP4 Protocol
- Dovecot POP3/IMAP Server
- Cyrus IMAP/POP3 Server
- Cyrus IMAP MTA Integration
- Cyrus Mailbox Administration
- Fetchmail
- Roundcube Webmail
- Mailing Lists
- GNU Mailman
- Mailman Configuration

Lab Tasks

- Configuring Procmal and SpamAssassin
- Configuring Cyrus IMAP
- Dovecot TLS Configuration
- Configuring Roundcube
- Base Mailman Configuration
- Basic Mailing List
- Private Mailing List

Appendix A - NIS

- NIS Overview
- NIS Limitations and Advantages
- NIS Client Configuration
- NIS Server Configuration
- NIS Troubleshooting Aids

Lab Tasks

- Using NIS for Centralized User Accounts
- Configuring NIS
- NIS Slave Server
- NIS Failover
- Troubleshooting Practice: NIS