

# Table of Contents

## RH253 Red Hat Network Services and Security Administration

### UNIT 1 — Introduction to System Services

Objectives	1-2
Agenda	1-3
Service Management	1-4
Services Managed by <code>init</code>	1-5
System V Service Management	1-6
<code>chkconfig</code>	1-7
<code>xinetd</code> Managed Services	1-8
The <code>xinetd</code> Daemon	1-9
<code>xinetd</code> default controls	1-10
<code>xinetd</code> service controls	1-11
The <code>/etc/sysconfig/</code> files	1-12
Fault Analysis	1-13
Security Enhanced Linux	1-14
SELinux	1-15
SELinux Installation Options and Control	1-16
Controlling SELinux	1-17
SELinux Contexts	1-18
Troubleshooting SELinux	1-19
End of Unit 1	1-20
<b>Lab: Introduction to System Services</b>	

### UNIT 2 — Organizing Networked Systems

Objectives	2-2
Agenda	2-3
Domain Name System(DNS)	2-4
Zones, Domains & Delegation	2-5
Name Server Hierarchy	2-6
The DNS Server	2-7
Berkeley Internet Name Domain (BIND)	2-8
Service Profile: DNS	2-9

<b>bind-choot</b>	2-10
Configuring BIND	2-11
Global Options	2-12
Address Control Lists (acl)	2-13
Name Daemon Control Utility ( <b>rndc</b> )	2-14
Master and Slave Zones	2-15
Reverse Lookup Zones	2-16
Special Zones	2-17
Zone Files	2-18
Resource Records (RR)	2-19
SOA (Start of Authority)	2-20
NS (Name Server)	2-21
Main Record Types	2-22
Example Zone File	2-23
Round Robin Load Sharing Through DNS	2-24
Delegating Subdomains	2-25
BIND Syntax Utilities	2-26
Caching-only Name Server	2-27
BIND Utilities	2-28
Advanced BIND Features	2-29
DHCP Overview	2-30
Service Profile: DHCP	2-31
Configuring a DHCP Server	2-32
End of Unit 2	2-33
<b>Lab: Organizing Networked Systems</b>	

### **UNIT 3 — Network File Sharing Services**

Objectives	3-2
Agenda	3-3
NFS File Service(NFS)	3-4
Service Profile: NFS	3-5
NFS Server	3-6
Client-side NFS	3-7
File Transfer Protocol (FTP)	3-8
Service Profile: FTP	3-9
Samba Services	3-10
Samba Daemons	3-11
Service Profile: SMB	3-12
Configuring Samba	3-13
Overview of <b>smb.conf</b> Sections	3-14
Configuring File and Directory Sharing	3-15
Printing to the Samba Server	3-16
Authentication Methods	3-17
Passwords	3-18

Samba Client Tools: <code>smbclient</code>	3-19
<code>nmblookup</code>	3-20
<code>smbmount</code>	3-21
Samba mounts in <code>/etc/fstab</code>	3-22
End of Unit 3	3-23
<b>Lab: Network File Sharing Services</b>	
<b>UNIT 4 Electronic Mail Services</b>	
Objectives	4-2
Agenda	4-3
Sendmail Features	4-4
Security and "Anti-Spam" Features	4-5
An Email Review	4-6
Server Operations	4-7
Service Profile: Sendmail	4-8
Main Configuration Files	4-9
Other Configuration Files	4-10
Sendmail Configuration with the <code>m4</code> Macro Language	4-11
Sendmail <code>m4</code> Macro File: Introduction	4-12
Sendmail <code>m4</code> Macro File: Features	4-13
Sendmail Client Configuration	4-14
Other Valuable <code>m4</code> directives	4-15
Additional Sendmail Configuration Files	4-16
<code>/etc/mail/virtusertable</code>	4-17
<code>/etc/mail/access</code>	4-18
Blacklisting Recipients	4-19
Debugging Sendmail	4-20
Using <code>alternatives</code>	4-21
Postfix	4-22
Service Profile: Postfix	4-23
Configuring Postfix	4-24
Additional Postfix Configuration	4-25
Enhanced Postfix Configuration	4-26
Procmail Local Delivery	4-27
Procmail Sample Configuration	4-28
End of Unit 4	4-29
<b>Lab: Electronic Mail Services</b>	
<b>UNIT 5 The HTTP Service</b>	
Objectives	5-2
Agenda	5-3
Apache Overview	5-4
Service Profile: HTTPD	5-5
Apache Configuration	5-6

Apache Server Configuration	5-7
Virtual Hosts	5-8
Apache Namespace Configuration	5-9
Apache Access Configuration	5-10
Using <code>.htaccess</code> Files	5-11
CGI	5-12
Notable Apache Modules	5-13
Apache Encrypted Web Server	5-14
Squid Web Proxy Cache	5-15
Service Profile: Squid	5-16
End of Unit 5	5-17
<b>Lab: The HTTP Service</b>	

## UNIT 6 — Security Concerns and Policy

Objectives	6-2
Agenda	6-3
Definition of Security	6-4
Attacks from the Network	6-5
Principles of Security	6-6
Security Practices	6-7
Diagnostic Utilities	6-8
Which Services Are Running?	6-9
Remote Service Detection	6-10
Isolate Vulnerabilities	6-11
Security Policy: the System	6-12
Security Policy: the People	6-13
Response Strategies	6-14
Additional Resources	6-15
End of Unit 6	6-16
<b>Lab: Security Concerns and Policy</b>	

## UNIT 7 — Authentication Services

Objectives	7-2
Agenda	7-3
User Authentication	7-4
Account Information	7-5
Name Service Switch	7-6
<code>getent</code>	7-7
Authentication	7-8
PAM	7-9
PAM Operation	7-10
<code>/etc/pam.d/</code> Files: Tests	7-11
<code>/etc/pam.d/</code> Files: Control Values	7-12

Example <code>/etc/pam.d/</code> File	7-13
<code>pam_stack</code>	7-14
<code>pam_unix</code>	7-15
Network Authentication	7-16
<code>auth</code> Modules	7-17
Password Security	7-18
Password Policy	7-19
<code>session</code> Modules	7-20
Utilities and Authentication	7-21
PAM Troubleshooting	7-22
NIS Overview	7-23
Service Profile: NIS	7-24
NIS Server Configuration	7-25
Configuring a Master Server	7-26
Configuring a Slave Server	7-27
NIS Client Configuration	7-28
NIS Troubleshooting	7-29
End of Unit 7	7-30
<b>Lab: Authentication Services</b>	

## UNIT 8 — System Monitoring

Objectives	8-2
Agenda	8-3
Introduction to System Monitoring	8-4
File System Analysis	8-5
Set User and Group ID Permissions	8-6
Typical Problematic Permissions	8-7
Ext2/3 Filesystem Attributes	8-8
System Log Files	8-9
<code>syslogd</code> and <code>klogd</code> Configuration	8-10
Advanced <code>syslogd</code> Configuration	8-11
Log File Analysis	8-12
Monitoring Processes	8-13
Process Monitoring Utilities	8-14
System Activity Reporting	8-15
Limiting Processes	8-16
Process Accounting Tools	8-17
End of Unit 8	8-18
<b>Lab: System Monitoring</b>	

## UNIT 9 — Securing Networks

Objectives	9-2
Agenda	9-3
IP Forwarding	9-4
Routing	9-5
Netfilter Overview	9-6
Netfilter Architecture	9-7
Netfilter Tables and Chains	9-8
Netfilter Packet Flow	9-9
Rule Matching	9-10
Rule Targets	9-11
Simple Example	9-12
Basic Chain Operations	9-13
Additional Chain Operations	9-14
Rules: General Considerations	9-15
Match Criteria (filter table)	9-16
TCP Match Extensions (filter table)	9-17
UDP and ICMP Match Extensions	9-18
Match Arguments	9-19
Chain Criteria	9-20
Directional Filtering I	9-21
Directional Filtering II	9-22
Connection Tracking	9-23
Connection Tracking Example	9-24
Network Address Translation(NAT)	9-25
SNAT Examples	9-26
DNAT Examples	9-27
Rules persistence	9-28
Example	9-29
End of Unit 9	9-30
<b>Lab: Securing Networks</b>	

## UNIT 10 — Securing Services

Objectives	10-2
Agenda	10-3
SystemV Startup Control	10-4
Securing the Service	10-5
<i>tcp_wrappers</i> Configuration	10-6
Daemon Specification	10-7
Client Specification	10-8
Advanced Syntax	10-9
Options	10-10
Example	10-11

Securing <code>xinetd</code> -managed services	10-12
<code>xinetd</code> Access Control	10-13
Host Patterns	10-14
Advanced Security Options	10-15
End of Unit 10	10-16
<b>Lab: Securing Services</b>	

## UNIT 11 — Securing Data

Objectives	11-2
Agenda	11-3
The Need For Encryption	11-4
Cryptographic Building Blocks	11-5
Random Numbers	11-6
One-Way Hashes	11-7
Symmetric Encryption	11-8
Asymmetric Encryption I	11-9
Asymmetric Encryption II	11-10
Public Key Infrastructures	11-11
Digital Certificates	11-12
Generating Digital Certificates	11-13
OpenSSH Overview	11-14
OpenSSH Authentication	11-15
The OpenSSH Server	11-16
Service Profile: SSH	11-17
OpenSSH Server Configuration	11-18
The OpenSSH Client	11-19
Protecting Your Keys	11-20
Applications: RPM	11-21
End of Unit 11	11-22
<b>Lab: Securing Data</b>	

## APPENDIX 1: Software Installation

# Table of Contents - Labs

Introduction to System Services	Lab 1
Organizing Networked Systems	Lab 2
Network File Sharing Services	Lab 3
Electronic Mail Services	Lab 4
The HTTP Service	Lab 5
Security Concerns and Policy	Lab 6
Authentication Services	Lab 7
System Monitoring	Lab 8
Securing Networks	Lab 9
Securing Services	Lab 10
Securing Data	Lab 11