

Linux Netzwerkadministration/ LPIC-2

Kurs 1002

© 2005-2012 OpenSource Training Ralf Spenneberg

Am Bahnhof 3-5

48565 Steinfurt

<http://www.opensource-training.de>

<http://www.os-t.de>

Copyright

Die in diesem Kurs zur Verfügung gestellten Folien, Unterlagen und Übungen sind urheberrechtlich geschützt. Wir behalten uns alle Rechte vor, auch die der fotomechanischen Wiedergabe und der Speicherung in elektronischen Medien. Die gewerbliche Nutzung ist nicht erlaubt.

Die Informationen in diesem Produkt werden ohne Rücksicht auf einen eventuellen Patentschutz veröffentlicht. Warennamen werden ohne Gewährleistung der freien Verwendbarkeit genutzt. Fast alle Hardware- und Softwarebezeichnungen, die in dieser Unterlage erwähnt werden, sind gleichzeitig auch eingetragene Warenzeichen.

Bei der Zusammenstellung der Texte und Abbildungen wurde mit größter Sorgfalt vorgegangen. Jedoch können Fehler nicht vollständig ausgeschlossen werden. Die Firma OpenSource Training Ralf Spenneberg kann für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Für Verbesserungsvorschläge und Hinweise auf Fehler sind wir dankbar.

Inhaltsverzeichnis

1	Einführung	7
1.1	IP-Adressen	7
1.1.1	Private IP-Adressen	9
1.1.2	Netzmasken	11
1.2	Dienste	13
1.2.1	Dienste steuern	13
1.2.2	Init-Prozess	15
1.2.3	System-V-Dienste	17
1.2.4	Runlevel verwalten	21
1.3	Xinetd	23
2	Netzwerkorganisation	31
2.1	DNS	31
2.1.1	Begriffsdefinitionen: Zonen, Domänen und Delegation	33
2.1.2	Ausfallsicherheit des DNS Protokolls	35
2.1.3	Caching Name Server	37
2.1.4	Globale Konfiguration	41
2.1.5	Sicherheit mit ACLs	43
2.1.6	Definition von Master- und Slave-Zonen	49
2.1.7	Reverse Lookup	51
2.1.8	Start of Authority	55
2.1.9	Nameserver Einträge	57
2.1.10	Lastverteilung	61
2.1.11	Fehlervermeidung und -suche	65
2.1.12	Client-Befehle zur Namensauflösung	67
2.2	DHCP	69
2.2.1	Einführung	69
2.2.2	Konfiguration	71
3	HTTP/FTP	73
3.1	Apache2	73
3.1.1	Konfiguration	77
3.1.2	Skalierung	79
3.1.3	Protokollierung	81
3.1.4	Namensauflösung	83
3.1.5	Webserver-Module	85
3.1.6	Virtual Hosting	87
3.1.7	Zugangsbeschränkungen	91
3.1.8	Authentifizierung der Benutzer	93
3.1.9	CGI und PHP - Programme anbieten	97
3.1.10	SSL Grundlagen	99

3.2	Vsftpd	101
3.2.1	Einführung VsFTP	101
3.2.2	Anonymes FTP	103
4	Proxy-Dienste: Squid	105
4.1	ACLs zur Zugriffssteuerung	107
4.2	Wichtige Parameter zur Konfiguratione	109
4.3	Authentifizierung der Benutzer	111
5	Samba/NFS	113
5.1	NFS	115
5.1.1	Definition von NFS-Freigaben im Server	115
5.1.2	NFSClient	117
5.2	Einführung Samba	119
5.2.1	Konfiguration	121
5.2.2	Freigaben	123
5.2.3	Drucken mit Samba	125
5.2.4	Authentifizierung der Benutzer	127
5.2.5	SMBClient	131
5.2.6	NMBLookup	133
5.2.7	Samba-Freigaben dauerhaft einbinden unter Linux	135
6	E-Mail	137
6.1	Postfix	137
6.1.1	Konfigurationsdateien für einen einfachen Mailserver	139
6.1.2	Postfachformate: Mbox - Maildir	147
6.1.3	Postfix Kommandos	149
6.2	Spamerkennung mit SpamAssassin	151
6.2.1	Einbindung über procmail	153
6.2.2	Konfiguration von SpamAssassin	155
7	Verschlüsselung	157
7.1	Geschichte der Verschlüsselung	157
7.2	Symmetrische Verschlüsselung	159
7.3	Asymmetrische Verschlüsselung	161
7.4	Hybridverfahren zur Verschlüsselung	163
7.5	X.509-Zertifikate	165
7.5.1	Zertifikate erzeugen	167
8	Secure Shell	169
8.1	Server-Konfiguration	171
8.2	SSH auf einem Client einsetzen	173
8.3	SSH-Schlüssel verwalten	175

9	TCP_Wrapper als einfache Firewall	177
9.0.1	Konfiguration	181
9.0.2	Wildcardcards	183
10	Zeitsynchronisation	185
10.1	Clientseitiger NTP-Daemon	187
10.2	NTP-Server	189
10.3	NTP Überwachung	191
11	Netzwerkbasierte Angriffe	193
11.1	Syn-Flood	193
11.2	SMURF-Angriff	195

Index

`/etc/resolv.conf`, 35

AES, 159

Apache2, 73

`.htaccess`, 95

 Authentifizierung, 93

 CGI, 97

 HostnameLookups, 83

`htpasswd`, 93

 Namensauflösung, 83

 Parameter

 AddType, 90

 Alias, 90

 Allow, 92

 Deny, 92

 DirectoryIndex, 90

 DocumentRoot, 87

 LoadModule, 85

 MaxClients, 79

 MaxRequestsPerChild, 79

 MaxSpareServers, 79

 MinSpareServers, 79

 Module, 85

 Order, 92

 ProxyRequest, 85

 ServerLimit, 79

 ServerSignature, 83

 ServerTokens, 83

 StartServers, 79

 UseCanonicalName, 83

 UserDir, 90

Perl, 97

PHP, 97

Protokollierung, 81

ServerName, 83

SSL, 99

Verzeichnisnamen, 89

Virtual Host, 87

Zugangsbeschränkungen, 91

Auto-Mounter, 117, 135

Bayes-Datenbank, 151

Bind 9, 39

Blowfish, 159

Body-Check, 151

Caching Name Server, 37

`chkconfig`, 21

CIDR, 11

Classless Internet Domain Routing, *siehe* CIDR

Cron-Daemon, 14

Dateien

`.htaccess`, 95

`/etc/dhcpd.conf`, 69

`/etc/exports`, 114

`/etc/fstab`, 117, 135

`/etc/mail/spamassassin/local.cf`, 155

`/etc/named.conf`, 40

`/etc/sysctl.conf`, 195

`/etc/vsftpd.ftputers`, 102

`/etc/vsftpd/vsftpd.conf`, 102

`/etc/xinetd.conf`, 27

`authorized_keys`, 175

`smb.conf`, 121

`ssl.conf`, 99

DES, 159

DHCP, 69

 Konfiguration, 71

`dhcp.leases`, 69

`dig`, 67

DNS, 31

 Ausfallsicherheit, 35

 Delegation, 33

 Domänen, 33

 Lastverteilung, 61

 Master-Server, 35

`named-checkconf`, 65

`named-checkzone`, 65

 Slave-Server, 35

 Zonen, 33

Zonendatei, 53
 DNS-Client-Befehle, 67
 Domain Name System, *siehe* DNS
 DSL, 9
 Dynamic Host Configuration Protocol, *siehe* DHCP
 FTP, *siehe* vsftpd
 Gateway, 7
 Header-Check, 151
 host, 67
 htpasswd, 93
 HTTP, *siehe* Apache2
 HTTP-Proxy, *siehe* Squid
 ifconfig, 7
 init, 14, 15
 -q, 16
 /etc/inittab, 16
 respawn, 16
 initctl, 17
 Internet Software Consortium, *siehe* ISC
 ip, 7
 IP-Adresse, 7
 private, 9
 ISC, 39, 69
 LDAP, 112
 libwrap, *siehe* TCP-Wrappers
 Linux-Dienste, 13
 Maildir, 147
 Master-Server, 35
 Mbox, 147
 Multi-Processing-Module, 74
 named-checkconf, 65
 named-checkzone, 65
 NAT, 9
 netmask, 7
 Network Address Translation, *siehe* NAT
 Network Time Protocol, 185
 Netzmaske, 7, 11

Netzwerkkonfiguration
 ifconfig, 7
 ip, 7
 route, 7
 NFS, 113
 nmblookup, 133
 nslookup, 67
 ntp, 185
 ntpd, 187, 189
 OpenSSH, 169
 PAM, 112
 Perl, 74
 PHP, 74
 Port
 443/tcp, 75, 99
 53/tcp, 40
 53/udp, 40
 67/udp, 69
 68/udp, 69
 80/tcp, 75
 953/tcp, 40
 Postfix, 137
 aliases, 139
 DMZ-Relay, 143
 Kommandos, 149
 postalias, 149
 postconf, 149
 postmap, 149
 postsuper, 149
 Konfigurationsverzeichnis, 139
 main.cf, 139
 master.cf, 139
 Parameter
 home_mailbox, 148
 mydestination, 141
 mydomain, 141
 myhostname, 141
 mynetworks, 141
 myorigin, 141
 pwcheck_method, 146
 relayhost, 141

- smtpd_recipient_restrictions, 141
- smtpd_sasl_application_name, 146
- smtpd_sasl_auth_enable, 146
- transport, 139
- Transport Map, 143
- virtual, 139
- Primary, 35
- private IP-Adressen, 9
- Private Key, 161
- Procmail, 153
- Public Key, 161
- RC4, 159
- RC5, 159
- RC6, 159
- rcservice, 20
- Reverse Lookup, 51
- RFC1918, 9
- route, 7
- Router, 7, 9
- Runlevel, 16, 17, 20, 21
- Samba, 112, 119
 - Authentifizierung, 127
 - Drucken, 125
 - Freigaben, 123
 - Kennwörter, 129
 - mount, 135
 - nmblookup, 133
 - Parameter
 - browseable, 125
 - comments, 125
 - cups options, 125
 - encrypt passwords, 128
 - guest ok, 125
 - load printers, 125
 - password server, 128
 - path, 125
 - printable, 125
 - printcap name, 125
 - printing, 125
 - realm, 128
 - workgroup, 128
- writable, 125
- smb.conf, 121
- smbclient, 131
- SASL, 145
- scp, 173
- Secondary, 35
- Serpent, 159
- service, 20
- sftp, 173
- Slave-Server, 35
- smbclient, 131
- Smurf-Angriff, 193
- SOA, 55
- SpamAssassin, 151
 - Konfiguration, 155
 - Parameter
 - body, 155
 - descripte, 155
 - report_safe, 155
 - required_hits, 155
 - rewrite_header, 155
 - score, 155
 - unwhitelist_from, 155
 - whitelist_from, 155
- Spare Server, 79
- Squid, 105
 - ACL, 107
 - Authentifizierung, 111
- SSH
 - Client, 173
 - scp, 173
 - sftp, 173
- ssh, 173
- ssh-agent, 175
- ssh-keygen, 175
- SSL, 74
- Start of Authority, *siehe* SOA
- Stratum, 191
- SYN-Cookie, 195
- SYN-Flood, 195
- System-V-Dienste, 19
- System-V-Skripte, 14

TCP-Wrappers, 25, 177, 179
Konfiguration, 181

UNC-Pfad, 131
upstart, 17

Venema, Wietse, 25, 137, 179
Verschlüsselung, 157
asymmetrisch, 161
hybrid, 163
symmetrisch, 159

Verteichnisse
/var/lib/dhcp/*, 69

Verzeichnisse
/etc/apache2/, 75
/etc/httpd/, 75
/etc/init.d/, 20
/etc/postfix/, 139
/etc/rc.d/*, 20
/etc/rndc.*, 40
/etc/xinetd.d/*, 23
/srv/www/, 75
/var/named/*, 40
/var/www/, 75

Virtual Host, 87

Virtual Hosting, 74

vsftpd, 101

anonym, 103

Parameter

anon_mkdir_write_enable, 103

anon_upload_enable, 103

anonymous_enable, 103

chown_uploads, 103

chown_username, 103

X.509, 165

Xinetd, 14, 23, 177

/etc/xinetd.conf, 27

/etc/xinetd.d/*, 23

access_time, 177

Authentifizierung, 25

max_load, 177

no_access, 177

only_from, 177

per_source, 177
Protokollierung, 25
Weiterleitung, 25

Zertifikat, 165
erzeugen, 167
Zonnendatei, 53