
Index

-
- .config, 239
- .d, 200
- .htaccess, 120
- /dev, 48
- /etc/apt/apt.conf.d/, 200
- /etc/apt/preferences, 202
- /etc/apt/sources.list, 178
- /etc/apt/trusted.gpg.d/, 208
- /etc/group, 112
- /etc/gshadow, 112
- /etc/network/interfaces, 109
- /etc/passwd, 112
- /etc/salt/minion, 261
- /etc/shadow, 112
- /etc/ssh/sshd_config, 115
- /proc, 48
- /sys, 48
- /var/lib/dpkg/, 217
- /var/www/html/, 118
- 32-bit CPU, 16
- 64-bit CPU, 16
- A**
- a2dismod, 118
- a2enmod, 118
- a2ensite, 119
- ACCEPT, 161
- account
 - creation, 112
 - disable, 113
 - modification, 113
- activity, monitoring, 168
- add a user to a group, 112
- addgroup, 113
- adduser, 112
- Advanced Package Tool, 177
- aide (Debian package), 170
- AllowOverride, Apache directive, 119, 120
- analysis
 - vulnerability, 6
 - web application, 6
- ansible, 261
- Apache, 118
 - directives, 119
- Apache directives, 121
- application assessments, 295
- applications
 - collection, 10
 - menu, 6
- applying a patch, 233
- apropos, 128
- APT, 177
 - configuration, 200
 - header display, 191
 - initial configuration, 84
 - interfaces, 196
 - package search, 191
 - pinning, 202
 - preferences, 202
- apt, 181
- apt build-dep, 231
- apt dist-upgrade, 185
- apt full-upgrade, 185
- apt install, 183
- apt purge, 186

- apt remove, 186
- apt search, 191
- apt show, 191
- apt source, 229
- apt update, 181
- apt upgrade, 184
- apt-cache, 191
- apt-cache dumpavail, 192
- apt-cache pkgnames, 192
- apt-cache policy, 192
- apt-cache search, 191
- apt-cache show, 191
- apt-cdrom, 178
- apt-get, 181
- apt-get dist-upgrade, 185
- apt-get install, 183
- apt-get purge, 187
- apt-get remove, 186
- apt-get update, 181
- apt-get upgrade, 184
- apt-key, 208
- apt-mark auto, 205
- apt-mark manual, 205
- apt-xapian-index, 192
- apt.conf.d/, 200
- aptitude, 181, 196
- aptitude dist-upgrade, 185
- aptitude full-upgrade, 185
- aptitude install, 183
- aptitude markauto, 205
- aptitude purge, 187
- aptitude remove, 186
- aptitude safe-upgrade, 184
- aptitude search, 191
- aptitude show, 191
- aptitude unmarkauto, 205
- aptitude update, 181
- aptitude why, 205
- architecture
 - multi-arch support, 206
- ARM installations, 98

- assessment
 - application, 295
 - black box, 296
 - formalization, 297
 - vulnerability, 288
 - white box, 296
- attacks
 - client side, 301
 - database, 6
 - denial of service, 298
 - memory corruption, 299
 - password, 7, 300
 - types of, 298
 - web, 300
 - wireless, 7
- auditing, security, 5
- authentication
 - package authentication, 208
- AuthName, Apache directive, 120
- AuthType, Apache directive, 120
- AuthUserFile, Apache directive, 120
- automatic installation, 95
- automatically installed packages, 205
- avalanche effect, 169
- axi-cache, 192

B

- background process, 57
- BackTrack, XXI, 2
- bash curly brackets, 168
- bash trick, 168
- bg, 57
- BIOS, 24
- block device file, 49
- boot preseed, 96
- boot screen, 67
- bootable USB key, 19
- bootloader, 85
- BOOTP, 258
- Breaks, header field, 214
- broken dependency, 195
- Bruce Schneier, 156

- brute-force attacks, 300
- buffer
 - overflow, 299
 - receive buffer, 162
- bug report, 134
- bugs.kali.org, 138
- build dependencies, installation, 231
- build options, 234
- Build-Depends, 231
- building
 - a custom live ISO image, 241
 - a package, 236
- C
- cache, proxy, 84
- cat, 56
- cd, 52
- cdimage.kali.org, 14, 181
- cdrom preseed, 96
- certification, 306
- chage, 113
- chain, 160
- changelog file, 271
- changelog.Debian.gz, 130
- character device file, 49
- checksecurity, 171
- checksums, 220
- chef, 261
- chfn, 113
- chgrp, 58
- chmod, 58
- choice
 - of country, 68
 - of language, 67
- chown, 58
- chroot, 245
- chsh, 113
- client side attacks, 301
- cluster, PostgreSQL cluster, 116, 117
- command line, 51
- communities, 132
- comparison of versions, 190

- compilation
 - of a kernel, 237
- compliance penetration test, 292
- component (of a repository), 179
- conffiles, 220
- confidentiality
 - files, 88
- config, debconf script, 220
- configuration
 - creating configuration packages, 269
 - files, 220
 - initial configuration of APT, 84
 - management, 261
 - network
 - DHCP, 71
 - static, 71
 - of the kernel, 239
 - program configuration, 114
- conflicts, 214
- Conflicts, header field, 214
- contrib, section, 179
- control, 211
- control file, 272
- control sum, 169
- control.tar.gz, 217
- copying, ISO image, 19
- copyright, 131
- copyright file, 271
- country selection, 68
- cp, 53
- createdb, 116
- createuser, 116
- creation
 - of a PostgreSQL database, 116
 - of a PostgreSQL user, 116
 - of groups, 113
 - of user accounts, 112
- credentials, default, 159
- cross-site scripting (XSS), 300
- cryptsetup, 248
 - nuke password, 250

- curly braces, 168
- customization of live ISO image, 241
- D**
- database assessment, 6
- database server, 115
- dch, 232
- dd, 22
- debconf, 220
- debconf-get, 101
- debconf-get-selections, 98
- debconf-set, 101
- DEBEMAIL, 270
- DEBFULLNAME, 270
- Debian
 - relationship with Kali Linux, 4
- Debian Administrator's Handbook, 307
- Debian Free Software Guidelines, 5
- Debian GNU/Linux, 2
- Debian Policy, 5
- debian-archive-keyring, 208
- debian-kernel-handbook, 238
- debian/changelog, 232, 271
- debian/control, 272
- debian/copyright, 271
- debian/patches, 230
- debian/rules, 234, 273
- debuild, 237
- default passwords, 159
- default.target, 122
- deletion of a group, 113
- delgroup, 113
- denial of service, 298
- dependency, 212
- Depends, header field, 212
- desktop environment, 3
 - choice during build of live ISO, 242
- desktop-base, 269
- detecting changes on the filesystem, 169
- device file, 49
- df, 60
- dh-make, 270

- dh_install, 273
- DHCP, 258
- dictionary attacks, 300
- directives, Apache, 119, 121
- DirectoryIndex, Apache directive, 120
- disable an account, 113
- disk preseed, 96
- Disks (program), 21
- diskutil, 23
- distribution, Linux, 2
- dm-crypt, 89
- dmesg, 60
- DNAT, 161
- dnsmasq, 258
- documentation, 128, 130
- download
 - ISO image, 14
 - the sources, 229
- dpkg, 176
 - database, 217
 - dpkg --verify, 169
 - internal operation, 219
- dpkg-buildpackage, 236
- dpkg-deb, 236
- dpkg-source --commit, 233
- drive, USB drive, 19
- DROP, 161
- dropdb, 116
- dropuser, 116
- dual boot, 87
- E**
- echo, 54
- editor, 56
- encrypted partition, 88
- encrypted persistence, 248
- engineering
 - reverse, 7
 - social engineering, 7
- Enhances, header field, 214
- environment
 - environment variable, 54

ExecCGI, Apache directive, 120
execution modules, salt, 262
execution, right, 57
experimental, 203
Explanation, 204
exploitation tools, 7

F

fail2ban, 158
features, 8
fg, 57
file
 confidentiality, 88
 configuration files, 220
file system, 49
filesystem
 hierarchy, 54
filtering rule, 160, 163
find, 56
fingerprint, 169
firewall, 159
FollowSymLinks, Apache directive, 120
forensics, 7
 mode, 8
formalization of the assessment, 297
format disk, 49
forums, 132
forums.kali.org, 132
FORWARD, 160
free, 60
Freenode, 133
fwbuilder, 166

G

get the sources, 229
getent, 112
git clone, 230
GitHub issues, 148
GNOME, 3
gnome-disk-utility, 21
gnome-system-monitor, 168
GNU

 Info, 130
gpasswd, 113
GPG key, 17
graphical.target, 122
grep, 56
group
 add a user, 112
 change, 113
 creation, 113
 deletion, 113
 of volumes, 89
 owner, 57
groupmod, 113
GRUB, 85
gui-apt-key, 210
guided partitioning, 76

H

hardware discovery, 61
heap corruption, 299
history of Kali Linux, 2
HOME, 55
home directory, 55
host, virtual host, 118
htpasswd, 121
HTTP proxy, 84
HTTP server, 118
http.kali.org, 180
HTTPS, 118
Hyper-V, 24

I

ICMP, 162
id, 60, 113
ifupdown, 109
impersonation, 7
Includes, Apache directive, 120
incompatibilities, 214
Indexes, Apache directive, 120
info, 130
information gathering, 6
initrd preseed, 96

- INPUT, 160
- installation, 66
 - automatic, 95
 - of build dependencies, 231
 - on ARM devices, 98
 - package installation, 182, 183
 - troubleshooting, 99
 - unattended, 95
- installer preseeding, 96
- integer overflow, 299
- Internet Control Message Protocol, 162
- ip6tables, 159, 163
- iptables, 159, 163
- IRC channel, 133
- isc-dhcp-server, 258
- ISO image
 - authentication, 17
 - booting, 24
 - copying, 19
 - custom build, 241
 - download, 14
 - mirrors, 14
 - variants, 16
- J**
- journal, 60
- journalctl, 60
- K**
- Kali Linux
 - communities, 132
 - documentation, 131
 - download, 14
 - features, 8
 - getting started, 14
 - history, 2
 - metapackages, 243
 - policies, 10
 - relationship with Debian, 4
 - repositories, 179
- kali-archive-keyring, 208
- kali-defaults, 269
- kali-dev, 4, 180
- kali-linux-* metapackages, 243
- kali-menu, 269
- kali-meta, 269
- kali-rolling, 4, 179
- kali.org/docs/, 131
- KDE, 3
- kernel, 48
 - compilation, 237
 - configuration, 239
 - logs, 60
 - sources, 238
- key
 - APT's authentication keys, 209
 - USB key, 19
- keyboard layout, 69
- kill, 57
- konqueror, 130
- KVM, 24
- L**
- language selection, 67
- layout, keyboard, 69
- less, 56
- libapache-mod-php, 118
- Linux, 48
 - distribution, 2
 - kernel, 2, 9
 - kernel sources, 238
- live ISO image, 14
 - custom build, 241
- live-boot, 245
- live-build, 241
 - adding files, 245
 - debconf preseeding, 244
 - hooks, 245
 - packages to install, 243
- loader
 - bootloader, 85
- LOG, 161
- logcheck, 167
- logging, 167

Logical Volume Manager, 89

login, remote login, 115

logs

- aptitude, 199

- dpkg, 194

- journal, 60

- kernel, 60

- monitoring, 167

ls, 52

lsdev, 61

lshw, 61

lspci, 61

lspcmcia, 61

lsusb, 61

LUKS, 89

LVM, 89

M

machine, virtual machine, 24

main, section, 179

make deb-pkg, 241

Makefile, 272

man, 128

management

- configuration management, 261

- of services, 121

manual pages, 128

manually installed packages, 205

mask

- rights mask, 59

MASQUERADE, 161

master boot record, 87

master, salt master, 261

MD5, 169

md5sums, 220

memory corruption, 299

menu, Kali Linux's applications menu, 6

metapackage, 213, 215

- kali-linux-*, 243

metapackages, 85

Metasploit Unleashed, 307

minion, salt minion, 261

mirrors, 14, 180

mkdir, 53

mkfs, 49

modification of a package, 228

modification, right, 57

monitoring, 167

- activity, 168

- files, 170

- log files, 167

more, 56

mount, 49

mount point, 82

Multi-Arch, 206

multi-user.target, 122

MultiViews, Apache directive, 120

mv, 53

N

netfilter, 159

network configuration, 71, 108

- with ifupdown, 109

- with NetworkManager, 108

- with systemd-network, 110

network installation, 258

network preseed, 97

network services, 10

- securing, 159

NetworkManager, 108

newgrp, 58, 113

NEWS.Debian.gz, 130

non-free, section, 179

nuke password, 250

O

octal representation of rights, 59

Offensive Security, 2

openssh-server, 115

Options, Apache directive, 119

OUTPUT, 160

overflow, buffer, 299

overlay filesystem, 246

owner

- group, 57
- user, 57

P

- package
 - authenticity check, 208
 - binary package, 176
 - build, 236
 - configuration, 269
 - conflict, 214
 - content inspection, 189
 - Debian package, 176
 - dependency, 212
 - file list, 187
 - header list, 190
 - incompatibility, 214
 - info, 190
 - installation, 182, 183
 - making changes, 232
 - meta-information, 210, 211
 - modification, 228
 - priority, 202
 - purge, 187
 - removal, 183, 186
 - replacement, 216
 - repository, 275
 - seal, 208
 - search, 188, 191
 - signature, 208
 - source of, 178
 - source package, 176
 - status, 188
 - unpacking, 182
 - version comparison, 190
 - virtual package, 215
- package tracker, 5
- Packages.xz, 178
- packaging
 - build options, 234
 - configuration packages, 269
 - new upstream version, 235
- packet
 - filter, 159
 - IP, 159
- PAE (Physical Address Extension), 36
- parted, 247
- partition
 - encrypted, 88
 - swap partition, 82
- partitioning, 75
 - guided partitioning, 75
 - manual partitioning, 79
- passwd, 113
- password, 113
 - attacks, 300
 - default passwords, 159
 - policy, 158
- password attacks, 7
- patch, 233
- patch application, 233
- PATH, 53
- PCI, 292
- penetration test
 - compliance, 292
 - traditional, 293
- penetration testing, 5
- penetration testing course, 307
- permissions, 57
- persistence, 246
 - encrypted, 248
 - multiple stores, 249
- pg_createcluster, 117
- pg_ctlcluster, 117
- pg_dropcluster, 117
- pg_hba.conf, 116
- pg_lsclusters, 117
- pg_renamecluster, 117
- pg_upgradecluster, 117
- PGP key, 17
- PHP, 118
- PID, process identifier, 50
- Pin, 204
- Pin-Priority, 204

- pininfo, 130
- ping, 162
- pinning, APT pinning, 202
- point, mount point, 82
- post exploitation, 7
- PostgreSQL, 115
- postinst, 217
- postrm, 217
- POSTROUTING, 160
- pre-dependency, 213
- Pre-Depends, header field, 213
- preferences, 202
- preinst, 217
- prerm, 217
- PREROUTING, 160
- presecd file, 97
- preseeding debian-installer, 96
- priority
 - package priority, 202
- program
 - configuration, 114
- Provides, header field, 215
- proxy, 84
- proxy cache, 84
- ps, 57
- puppet, 261
- purge of a package, 187
- purging a package, 187
- pwd, 52
- PXE boot, 258

Q

- QCOW, 30
- QEMU, 24

R

- read, right, 57
- README.Debian, 130
- receive buffer, 162
- Recommends, header field, 214
- REDIRECT, 161
- redirection, 56

- reinstallation, 194
- REJECT, 161
- Release.gpg, 208
- remote login, 115
- removal of a package, 183
- removing a package, 186
- replacement, 216
- Replaces, header field, 216
- report a bug, 134
- reportbug, 143
- reporting tools, 7
- repository of packages, 275
- reprepro, 275
- Require, Apache directive, 121
- requirements, minimal installation require-
ments, 66
- rescue mode of installer, 87
- resize a partition, 80
- retrieve the sources, 229
- reverse engineering, 7
- rights, 57
 - mask, 59
 - octal representation, 59
- risk model, 156
- risk ratings, 290
- rkhunter, 171
- rm, 53
- rmdir, 53
- Rolling, Kali Rolling, 3
- root password, 159
- RTFM, 128
- rules file, 273

S

- salt execution modules, 262
- salt formulas, 264
- salt state modules, 265
- salt states, 264
- salt-key, 261
- saltstack, 261
- samhain, 170
- scanning threads, 290

- Schneier, Bruce, 156
- search of packages, 191
- section
 - contrib, 179
 - main, 179
 - non-free, 179
- secure boot, 24
- secure ssh, 159
- securing, 156
 - a laptop, 158
 - a server, 158
 - network services, 159
- security
 - assessments, 284
 - auditing, 5
 - policy, 156
- service file, systemd service file, 122
- services management, 121
- setgid directory, 58
- setgid, right, 58
- setuid, right, 58
- Setup, 24
- sg, 113
- SHA1, 169
- SHA256SUMS, 17
- shell, 52
- shrink a partition, 80
- signal, 57
- signature
 - package signature, 208
- SNAT, 161
- sniffing, 7
- social engineering tools, 7
- source
 - of packages, 178
 - of the Linux kernel, 238
 - package, 176
 - retrieval, 229
- source package
 - build, 236
 - making changes, 232
- sources.list, 178
- Sources.xz, 178
- spoofing, 7
- SQL injection, 300
- SSH, 115
- ssh service, 159
- SSL, 118
- state modules, salt, 265
- sticky bit, 58
- sudo, 109
- Suggests, header field, 214
- swap, 82
- swap partition, 82
- SymLinksIfOwnerMatch, Apache directive, 120
- synaptic, 196, 199
- system administration, 307
- system, file system, 49
- systemctl, 121
- systemd, 121
- systemd-network, 110
- systemd-resolved, 111

T

- target, systemd target, 122
- TFTP, 258
- tftpd-hpa, 258
- threat model, 156
- TLS, 118
- top, 168
- tracker
 - package tracker, 5
- traditional penetration test, 293
- training, 306
- tripwire, 170
- troubleshooting installations, 99
- trust, web of trust, 18
- trusted key, 209

U

- UEFI, 24
- ULOG, 161
- umask, 59

- uname, 60
- unattended installation, 95
- union mount, 246
- unit, systemd unit, 121
- unpacking
 - binary package, 182
- upgrade
 - handling problems after an upgrade, 193
 - system upgrade, 184
- upstream version, packaging a new one, 235
- USB key, 19
- user
 - owner, 57
- user creation, 72
- user space, 48

V

- variable, environment, 54
- variants of live ISO image, 242
- VDI, 30
- version, comparison, 190
- vigr, 112
- vipw, 112
- virtual host, 118
- virtual machine, 24
- virtual memory, 82
- virtual package, 215
- VirtualBox, 24
- VMware, 24
- volume
 - group, 89
 - logical volume, 89
 - physical volume, 89
- vulnerability
 - analysis, 6
 - assessments, 288
 - client side, 301
 - denial of service, 298
 - memory corruption, 299
 - password, 300
 - scans, 290
 - types of, 298

- web, 300

W

- WantedBy, systemd directive, 122
- Wants, systemd directive, 122
- web access restriction, 121
- web application analysis, 6
- web attacks, 300
- web authentication, 120
- web of trust, 18
- web server, 118
- Win32 Disk Imager, 19
- wireless attacks, 7
- write, right, 57

X

- XDG, 55
- Xen, 24
- Xfce, 3

Y

- yelp, 130