O AUTORU

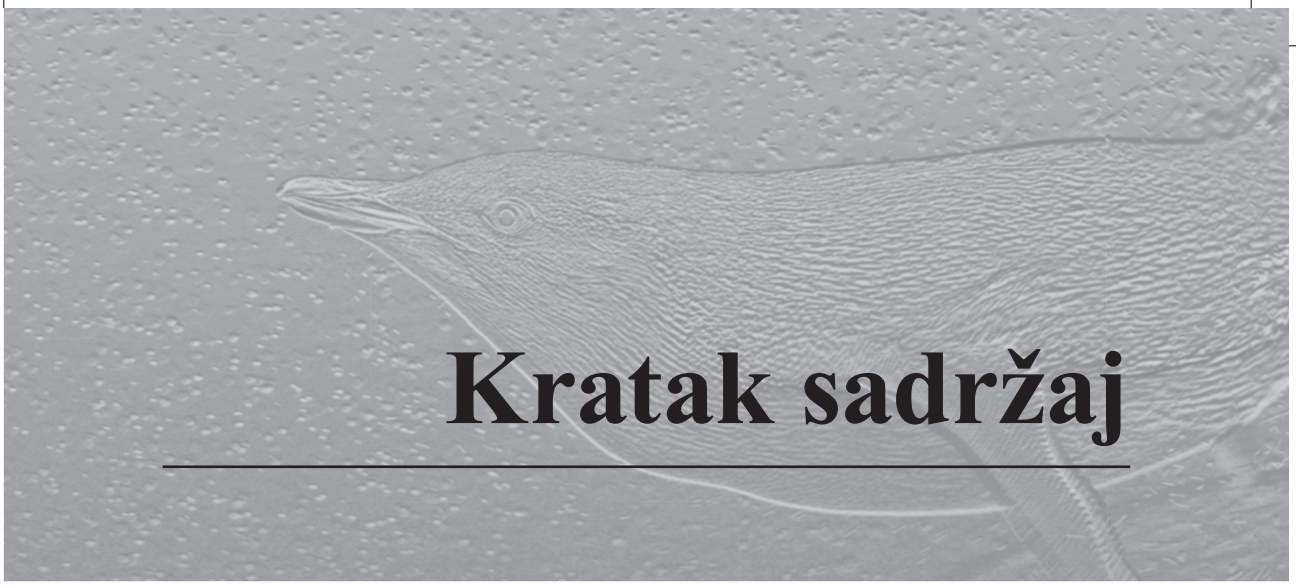
Rob Van den Brink je konsultant kompanije „Coherent Security“ u Ontariju, u Kanadi. Volonter je na sajtu Internet Storm Center koji svakodnevno objavljuje blogove o bezbednosti informacija i srodne priče. Rob takođe doprinosi kao volonter različitim bezbednosnim benčmarkovima u Centru za bezbednost na Internetu, posebno benčmarkovima Palo Alto Networks Firewall i Cisco Nexus.

Njegove oblasti specijalizacije obuhvataju sve aspekte informacione bezbednosti, mrežne infrastrukture, projektovanja mreže i centra podataka, IT automatizaciju, orkestraciju i virtuelizaciju. Rob je razvio alatke za obezbeđivanje usaglašenosti smernica za korisnike sa pristupom VPN-u, razne mrežne alatke koje su izvorne za Cisco IOS, kao i alatke za reviziju/procenu bezbednosti za Palo Alto Networks Firewall i VMware vSphere.

Rob je stekao master diplomu iz inženjeringa informacione bezbednosti na Institutu za tehnologiju SANS i poseduje niz SANS/GIAC, VMware i Cisco sertifikata.

O RECENZENTU

Melvin Reyes Martin je entuzijastični viši inženjer umrežavanja, koji je pasionirani ljubitelj dizajna, poboljšavanja i automatizacije. Stekao je sertifikate na nivou stručnjaka za umrežavanje, kao što su CCIE Enterprise Infrastructure i CCIE Service Provider. Radio je u kompaniji „Cisco Systems“ šest godina na implementiranju novih uzbudljivih mrežnih tehnologija za dobavljače internet usluga u regionima Latinske Amerike i Kariba. Osim toga, poseduje Linux+ sertifikat i voli da integriše projekte otvorenog koda u umrežavanje. Melvin je veliki zagovornik infrastrukture u „oblaku“ i blokčejn (blockchain) tehnologije.



Kratak sadržaj

PREDGOVOR . . . . . **XIX**

DEO I

Osnove Linuxa **1**

POGLAVLJE 1

Dobrodošli u Linux porodicu! **3**

POGLAVLJE 2

Osnovna Linux mrežna konfiguracija i operacije – korišćenje lokalnih interfejsa **17**

DEO II

Linux kao mrežni čvor i platforma za rešavanje problema **41**

POGLAVLJE 3

Korišćenje Linuxa i Linux alatki za dijagnostiku mreže **43**

POGLAVLJE 4

Linux firewall **97**

POGLAVLJE 5

Linux bezbednosni standardi sa primerima iz stvarnog života **115**

DEO III

Linux mrežne usluge 149

POGLAVLJE 6
DNS usluge na Linuxu 151

POGLAVLJE 7
DHCP usluge u Linuxu 181

POGLAVLJE 8
Sertifikacione usluge u Linuxu 199

POGLAVLJE 9
RADIUS usluge za Linux 227

POGLAVLJE 10
Usluge balansera opterećenja za Linux 265

POGLAVLJE 11
Hvatanje i analiza paketa u Linuxu 299

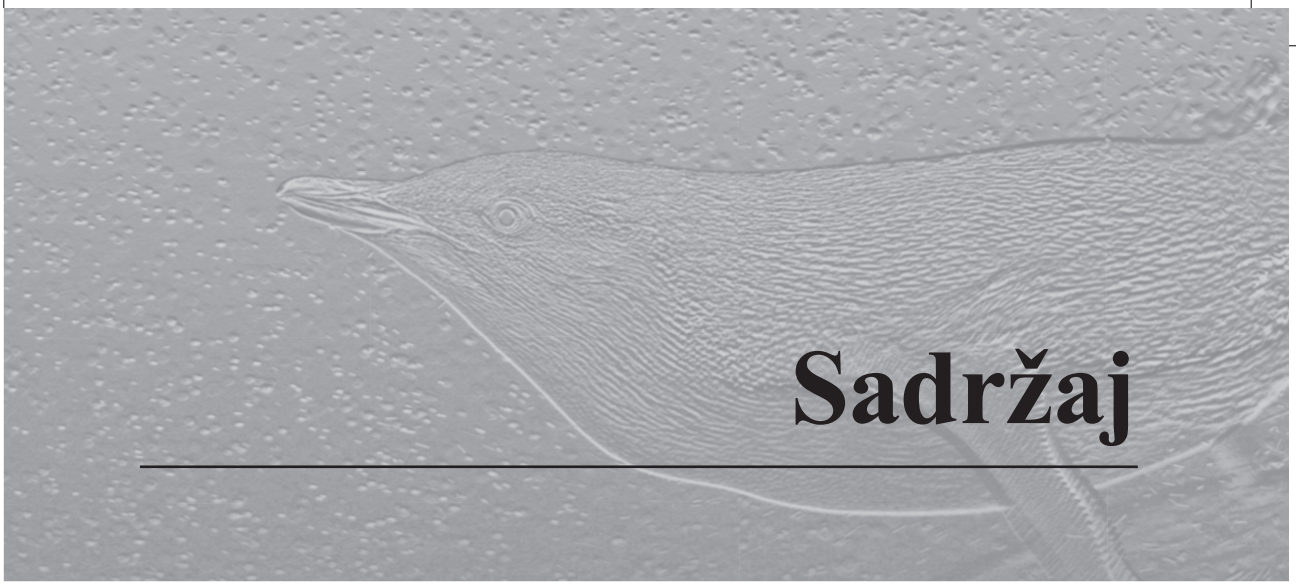
POGLAVLJE 12
Nadzor mreže pomoću Linuxa 335

POGLAVLJE 13
Sistemi za sprečavanje upada u Linuxu 397

POGLAVLJE 14
Honeypot usluge u Linuxu 441

PROCENE 473

INDEKS 491



Sadržaj

PREDGOVOR XIX

DEO I

Osnove Linuxa 1

POGLAVLJE 1

Dobrodošli u Linux porodicu! 3

Zašto je Linux dobar za tim umrežavanja 4
Zašto je Linux važan? 5
Istorija Linuxa 7
Mainstream data center Linux 8
Red Hat 8
Oracle/Scientific LinuX 9
SUSE 9
Ubuntu 9
BSD/FreeBSD/OpenBSD 10
Specijalne Linux distribucije 10
Firewallovi otvorenog koda 11
Kali Linux 11
SIFT 11
Security Onion 11
Virtuelizacija 12
Linux i računarstvo u „oblaku“ 12
Odabir Linux distribucije za vašu organizaciju 13
Zaključak 14
Pročitajte još 14

POGLAVLJE 2

Osnovna Linux mrežna konfiguracija i operacije – korišćenje lokalnih interfejsa 17

Tehnički zahtevi 18
Korišćenje mrežnih postavki – dva skupa komandi 18
Prikaz informacija o IP adresi interfejsa 21
Prikaz informacija o rutiranju 24
IPv4 adrese i maske podmreža 26
Adrese posebne namene 27
Privatne adrese – RFC 1918 29
Dodeljivanje IP adrese interfejsu 30
Dodavanje rute 32
Dodavanje rute korišćenjem starih pristupa 34
Onemogućavanje i omogućavanje interfejsa 34
Podešavanje MTU-a na interfejsu 35
Više o komandi nmcli 36
Rezime 39
Pitanja 39
Pročitajte još 39

DEO II

Linux kao mrežni čvor i platforma za rešavanje problema 41

POGLAVLJE 3

Korišćenje Linuxa i Linux alatki za dijagnostiku mreže 43

Tehnički zahtevi 44
Osnove mreže – OSI model 45
Sloj 2 – povezivanje IP i MAC adresa pomoću ARP-a 47
OUI vrednosti MAC adrese 53
Sloj 4 – kako funkcionišu TCP i UDP portovi 54
Sloj 4 TCP i trostepeno usaglašavanje 55
Enumeracija lokalnog porta – na šta sam povezan? Šta osluškujem? 57
Enumeracija udaljenih portova pomoću izvornih alatki 68
Enumeracija udaljenih portova i usluga – nmap 74
NMAP skriptovi 82
Da li postoje ograničenja za Nmap? 88
Bežične dijagnostičke operacije 89
Rezime 95
Pitanja 96
Pročitajte još 96

POGLAVLJE 4

Linux firewall. 97

Tehnički zahtevi 98
Konfigurisanje iptablesa 98
iptables sa visokog nivoa 99
NAT tabela 105
Mangle tabela 107
Redosled operacija u iptablesu 108
Konfigurisanje nftablesa 110
nftables osnovna konfiguracija 111
Korišćenje datoteka include 112
Uklanjanje konfiguracije firewalla 113
Rezime 113
Pitanja 114
Pročitajte još 114

POGLAVLJE 5

Linux bezbednosni standardi sa primerima iz stvarnog života. 115

Tehnički zahtevi 116
Zašto moram da zaštitim svoje Linux hostove? 116
Razmatranja o bezbednosti specifičnoj za „oblak“ 117
Uobičajeni bezbednosni standardi specifični za softversku industriju 118
Kritične kontrole Centra za bezbednost na Internetu 119
Početak upotrebe kritičnih bezbednosnih kontrola za CIS 1 i 2 123
Kritična kontrola 1 – popis hardvera 123
Kritična kontrola 2 – popis softvera 128
OSQuery – kritične kontrole 1 i 2 i dodavanje kontrola 10 i 17 131
Benčmarkovi Centra za bezbednost na Internetu 136
Primena CIS benčmarka – zaštita SSH-a na Linuxu 137
Ensure SSH root login is disabled (5.2.9) 139
SELinux i AppArmor 144
Rezime 146
Pitanja 146
Pročitajte još 147

DEO III

Linux mrežne usluge 149

POGLAVLJE 6

DNS usluge na Linuxu 151

Tehnički zahtevi 152
Šta je DNS? 152
Dve glavne implementacije DNS servera 153

„Interni" DNS server organizacije (i pregled DNS-a) ... 153
DNS server u internet okruženju ... 157
Uobičajene DNS implementacije ... 159
Osnovna instalacija: BIND za internu upotrebu ... 159
BIND: Specifičnosti implementacije u internet okruženju ... 163
Rešavanje DNS problema i izviđanje ... 165
DoH ... 166
DoT ... 169
knot-dnsutils ... 171
Implementacija DoT-a u Nmapu ... 174
DNSSEC ... 175
Rezime ... 177
Pitanja ... 177
Pročitaje još ... 177

POGLAVLJE 7

DHCP usluge u Linuxu ... 181

Kako funkcioniše DHCP? ... 181
Osnovni DHCP rad ... 182
DHCP zahtevi iz drugih podmreža (prosleđivači, releji ili pomoćnici) ... 183
DHCP opcije ... 185
Zaštita DHCP usluga ... 187
Zlonamerni DHCP server ... 187
Zlonamerni DHCP klijent ... 190
Instaliranje i konfigurisanje DHCP servera ... 191
Osnovna konfiguracija ... 191
Statičke rezervacije ... 194
Jednostavno DHCP evidentiranje i rešavanje problema u njegovoj svakodnevnoj upotrebi ... 195
Rezime ... 197
Pitanja ... 198
Pročitajte još ... 198

POGLAVLJE 8

Sertifikacione usluge u Linuxu ... 199

Tehnički zahtevi ... 200
Šta su sertifikati? ... 200
Dobijanje sertifikata ... 201
Korišćenje sertifikata – primer veb servera ... 204
Izrada privatnog izdavaoca sertifikata ... 208
Izrada CA pomoću OpenSSL-a ... 208
Zahtevanje i potpisivanje CSR-a ... 212
Zaštita infrastrukture izdavaoca sertifikata ... 215
Nasleđeni isprobani i dobri saveti ... 215
Savremeni savet ... 215

Rizici specifični za CA u savremenim infrastrukturama ... 216
Transparentnost sertifikata ... 217
Korišćenje CT-a za popis ili izviđanje ... 218
Automatizacija izdavanja sertifikata i ACME protokol ... 219
OpenSSL podsetnik (cheat sheet) ... 221
Rezime ... 224
Pitanja ... 224
Pročitajte još ... 224

POGLAVLJE 9

RADIUS usluge za Linux ... 227

Tehnički zahtevi ... 228
RADIUS osnove – šta je RADIUS i kako funkcioniše? ... 228
Implementacija RADIUS-a sa lokalnom Linux autentikacijom ... 232
RADIUS sa LDAP/LDAPS pozadinskom autentikacijom ... 234
NTLM autentikacija (AD) – uvod u CHAP ... 239
Unlang – unlanguage ... 246
Scenariji upotrebe RADIUS-a ... 247
VPN autentikacija pomoću korisničkog ID-a i lozinke ... 248
Administrativni pristup mrežnim uređajima ... 249
Administrativni pristup ruterima i prekidačima ... 250
RADIUS konfiguracija za EAP-TLS autentikaciju ... 252
Provera autentičnosti bežične mreže pomoću 802.1x/EAP-TLS-a ... 254
Provera autentičnosti ožičene mreže pomoću 802.1x/EAP-TLS-a ... 257
Upotreba Google Authenticatora za MFA pomoću RADIUS-a ... 260
Rezime ... 261
Pitanja ... 262
Pročitajte još ... 262

POGLAVLJE 10

Usluge balansera opterećenja za Linux ... 265

Tehnički zahtevi ... 266
Uvod u raspoređivanje opterećenja ... 266
Round Robin DNS (RRDNS) ... 266
Dolazni proksi – raspoređivanje opterećenja sloja7 ... 268
Dolazni NAT – raspoređivanje opterećenja sloja 4 ... 270
DSR raspoređivanje opterećenja ... 272
Specifične postavke servera za DSR ... 274
Algoritmi za raspoređivanje opterećenja ... 275
Provere ispravnosti servera i usluga ... 276
Razmatranje dizajna balansera opterećenja centra podataka ... 277
Razmatranja o mreži i upravljanju centrima podataka ... 280
Izrada HAProxy NAT/proxy balansera opterećenja ... 284
Pre konfiguracije – NIC-ovi, adresiranje i rutiranje ... 285

Pre konfiguracije – fino podešavanje performansi ... 285
TCP usluge raspoređivanja opterećenja – veb usluge ... 287
Postavljanje trajnih (lepljivih) veza ... 291
Napomena o implementaciji ... 292
HTTPS frontending ... 292
Završna reč o bezbednosti balansera opterećenja ... 295
Rezime ... 296
Pitanja ... 297
Pročitajte još ... 297

POGLAVLJE 11

Hvatanje i analiza paketa u Linuxu ... 299

Tehnički zahtevi ... 300
Uvod u hvatanje paketa – prava mesta za traženje ... 300
Hvatanje sa oba kraja ... 300
Prebacivanje porta za nadzor ... 301
Posredni unutrašnji host ... 302
Network tap ... 302
Pristupi zlonamernog hvatanja paketa ... 304
Razmatranje performansi prilikom hvatanja ... 307
Alatke za hvatanje ... 309
tcpdump ... 309
Wireshark ... 309
TShark ... 310
Druge PCAP alatke ... 310
Filtriranje uhvaćenog saobraćaja ... 310
Wireshark filteri za hvatanje (hvatanje saobraćaja kućne mreže) ... 311
tcpdump filteri za hvatanje – VoIP telefoni i DHCP ... 313
Više filtera za hvatanje – LLDP i CDP ... 318
Prikupljanje datoteka iz hvatanja paketa ... 321
Rešavanje problema aplikacije – snimanje VoIP telefonskog poziva ... 324
Wireshark filteri za prikaz – odvajanje određenih podataka u snimanju ... 330
Rezime ... 333
Pitanja ... 333
Pročitajte još ... 334

POGLAVLJE 12

Nadzor mreže pomoću Linuxa ... 335

Tehnički zahtevi ... 336
Evidentiranje pomoću Sysloga ... 336
Veličina evidencije, rotiranje i baze podataka ... 337
Analiza evidencije – pronalaženje „stvari“ ... 338
Gde tražiti? ... 338
Kako pretraživati? ... 338

Upozorenja o određenim događajima ... 340
Primer Syslog servera – Syslog ... 342
Projekat Dshield ... 348
Upravljanje mrežnim uređajima pomoću SNMP-a ... 351
Osnovni SNMP upiti ... 352
Primer primene SNMP NMS-a – LibreNMS ... 356
Specifičnosti hipervizora ... 357
Podešavanje osnovnog SNMPv2 uređaja ... 359
SNMPv3 ... 363
Upozorenja ... 366
Šta treba da imate na umu dok dodajete uređaje? ... 369
Usluge nadgledanja ... 369
Prikupljanje NetFlow podataka na Linuxu ... 373
Šta su NetFlow i njegovi „rođaci" SFLOW, J-Flow i IPFIX? ... 373
Koncepti implementacije prikupljanja tokova ... 375
Konfigurisanje rutera ili sviča za prikupljanje tokova ... 376
Primer NetFlow servera koji koristi NFDump i NFSen ... 379
Druge NetFlow alternative otvorenog koda ... 390
Komercijalne ponude ... 391
Rezime ... 391
Pitanja ... 392
Pročitajte još ... 392
Često korišćeni SNMP OID-ovi ... 394

POGLAVLJE 13

Sistemi za sprečavanje upada u Linuxu 397

Tehnički zahtevi ... 398
Šta je IPS? ... 398
Opcije arhitekture – gde se IPS uklapa u vaš centar podataka? ... 399
IPS tehnike izbegavanja ... 404
Otkrivanje WAF-a ... 404
Fragmentacija i drugi metodi izbegavanja IPS-a ... 405
Klasična/mrežna IPS rešenja – Snort i Suricata ... 407
Suricata IPS primer ... 408
Konstruisanje IPS pravila ... 420
Pasivno praćenje saobraćaja ... 424
Pasivno praćenje pomoću alatke P0F – primer ... 425
Zeek primer – prikupljanje mrežnih metapodataka ... 427
Rezime ... 437
Pitanja ... 438
Pročitajte još ... 438

POGLAVLJE 14

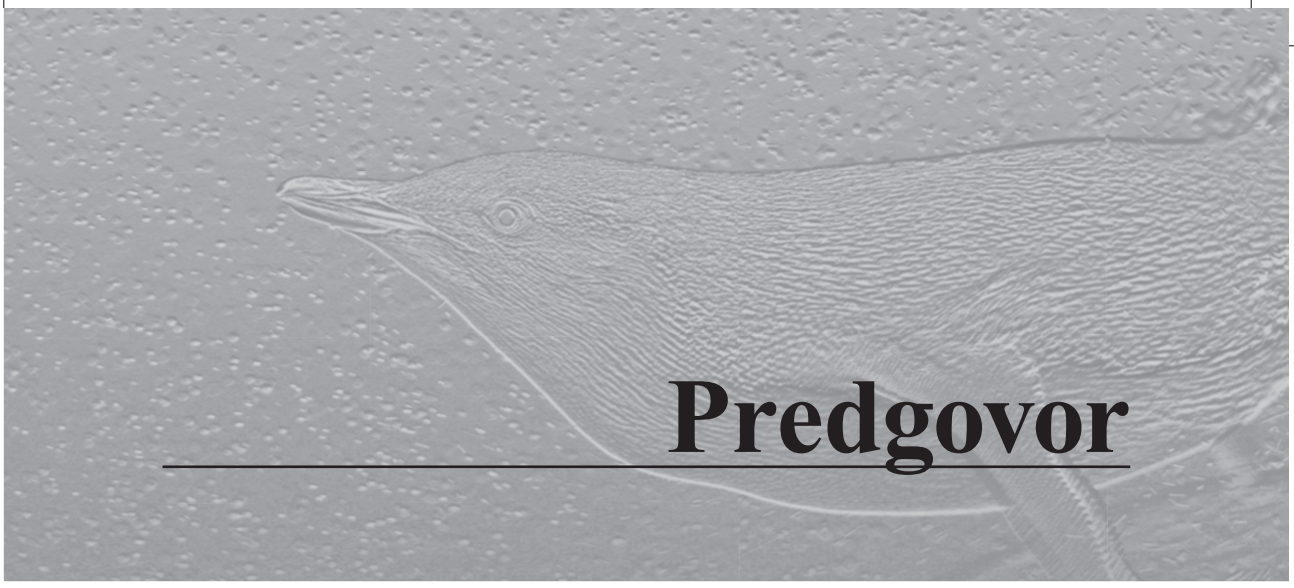
Honeypot usluge u Linuxu 441

Tehnički zahtevi 442
Pregled honeypota – šta je honeypot i zašto ga želim? 442
Scenariji postavljanja i arhitektura – gde da stavim honeypot? 444
Rizici primene honeypotova 449
Primeri honeypotova 450
Osnovni honeypotovi za upozoravanje portova – iptables, netcat i portspoof 450
Drugi uobičajeni honeypotovi 455
Distribuirani/zajednički honeypot – DShield Honeypot projekat Internet Storm Centera 456
Rezime 470
Pitanja 470
Pročitajte još 471

PROCENE 473

Poglavlje 2 - Osnovna Linux mrežna konfiguracija i operacije – korišćenje lokalnih interfejsa 473
Poglavlje 3 - Korišćenje Linuxa i Linux alatki za dijagnostiku mreže 474
Poglavlje 4 – Linux firewall 476
Poglavlje 5 - Linux bezbednosni standardi sa primerima iz stvarnog života 477
Poglavlje 6 - DNS usluge u Linuxu 478
Poglavlje 7 – DHCP usluge u Linuxu 478
Poglavlje 8 – Sertifikacione usluge u Linuxu 482
Poglavlje 9 – RADIUS usluge u Linuxu 484
Poglavlje 10 – Usluge balansiranja opterećenja za Linux 485
Poglavlje 11 - Hvatanje i analiza paketa u Linuxu 486
Poglavlje 12 - Nadzor mreže pomoću Linuxa 487
Poglavlje 13 - Sistemi za sprečavanje upada u Linuxu 488
Poglavlje 14 – Honeypot usluge u Linuxu 490

INDEKS 491



Predgovor

Dobrodošli u Linux za profesionalce umrežavanja! Ako ste se ikada zapitali kako da smanjite troškove hostova i usluga koje podržavaju vašu mrežu, došli ste na pravo mesto. Ili ako razmišljate kako da počnete da obezbeđujete mrežne usluge, kao što su DNS, DHCP ili RADIUS, možemo vam pomoći i na tom putu.

Postoji usluga koja vam pomaže da podržite vašu mrežu - pokušaćemo da objasnimo kako da je pokrenete korišćenjem osnovne konfiguracije, kao i da vam pomognemo da započnete zaštitu te usluge. Usput ćemo pokušati da vam pomognemo da odaberete Linux distribuciju, da vam pokažemo kako da koristite Linux za rešavanje problema i da upoznate nekoliko usluga za koje možda niste znali da su vam potrebne.

Nadamo se da će vam „put“ na koji ćete krenuti u ovoj knjizi pomoći da dodate nove usluge vašoj mreži, a možda i da bolje upoznate vašu mrežu!

Kome je namenjena ova knjiga

Ova knjiga je namenjena onima koji imaju zadatak da upravljaju mrežnom infrastrukturom bilo koje vrste. Ako ste zainteresovani za detalje o načinu funkcionisanja „stvari“ u vašoj mreži, ova knjiga je za vas! Naše razmatranje će vam takođe biti zanimljivo ako se često pitate kako ćete isporučiti različite usluge na vašoj mreži koje su potrebne vašoj organizaciji, ali možda nemate budžet za plaćanje komercijalnih proizvoda. Razmotrićemo kako funkcioniše svaka od Linux usluga o kojima govorimo i kako ih možete konfigurisati u tipičnom okruženju.

Na kraju, ako ste zabrinuti zbog toga kako napadači vide vaše mrežne resurse, pronaći ćete mnogo štošta što će vas zanimati! Razmotrićemo kako napadači i zlonamerni softver (malwer) obično napadaju različite usluge na vašoj mreži i kako da odbranite te usluge.

Pošto je naš fokus u ovoj knjizi na Linuxu, videćete da se budžet za primenu i odbranu usluga koje razmatramo meri vašim entuzijazmom i vremenom za učenje novih i zanimljivih „stvari“, a ne dolarima i centima!

Šta obuhvata ova knjiga

Poglavlje 1, „Dobrodošli u Linux porodicu!“, sastoji se od kratke istorije Linuxa i opisa različitih Linux distribucija. Osim toga, nudimo nekoliko saveta za izbor Linux distribucije za vašu organizaciju.

U Poglavlju 2, „Osnovna Linux mrežna konfiguracija i operacije – korišćenje lokalnih interfejsa“, razmatramo konfiguraciju mrežnog interfejsa u Linuxu, koja može da bude pravi kamen spoticanja za mnoge administratore, posebno kada je doneta odluka da serveru nije potreban GUI. U ovom poglavlju ćemo razmotriti kako da konfigurišemo različite parametre mrežnog interfejsa iz komandne linije, kao i mnogo osnova o IP i MAC slojevima.

Poglavlje 3, „Korišćenje Linuxa i Linux alatki za dijagnostiku mreže“, sadrži dijagnostikovanje i rešavanje problema sa mrežom, što je svakodnevni posao za skoro sve administratore mreža. U ovom poglavlju nastavićemo istraživanje koje smo započeli u prethodnom poglavlju i nadovezaćemo se na osnove TCP-a i UDP-a. Nakon toga, razmotrićemo dijagnostiku lokalne i udaljene mreže korišćenjem izvornih Linux komandi, kao i uobičajenih programskih dodataka. Završićemo ovo poglavlje razmatranjem pristupa bežičnim mrežama.

U Poglavlju 4, „Linux firewall“, objašnjeno je da Linux firewall može da bude pravi izazov za mnoge administratore, posebno zato što postoji više različitih „generacija“ implementacije firewalla iptables/ipchains. Razmotrićemo evoluciju Linux firewalla i primenićemo ga da bismo zaštitili određene usluge u Linuxu.

Poglavlje 5, „Linux bezbednosni standardi sa primerima iz stvarnog života“, obuhvata zaštitu Linux hosta, koji je uvek pokretna meta, u zavisnosti od usluga implementiranih na tom hostu i okruženja u kojem je primenjen. Razmotrićemo ove izazove, kao i razne bezbednosne standarde koje možete da koristite za donošenje bezbednosnih odluka. Posebno ćemo razmotriti kritične kontrole **Center for Internet Security (CIS)** i nekoliko preporuka u CIS Benchmarku za Linux.

U Poglavlju 6, „DNS usluge u Linuxu“, objašnjeno je kako DNS funkcioniše u različitim instancama i kako da implementirate DNS usluge u Linuxu, kako interno tako i na Internetu. Takođe će biti reči o raznim napadima na DNS i načinima zaštite servera od njih.

Poglavlje 7, „DHCP usluge u Linuxu“, sadrži DHCP, koji se koristi za izdavanje IP adresa klijentskim radnim stanicama, kao i za „guranje“ mnoštva opcija

konfiguracije na klijentske uređaje svih vrsta. U ovom poglavlju ćemo prikazati kako se implementiraju DHCP usluge na Linux za tradicionalne radne stanice i razmotriti ono što treba da uzmete u obzir za druge uređaje, kao što su telefoni Voice over IP (VoIP).

Poglavlje 8, „Sertifikacione usluge u Linuxu“, posvećeno je sertifikatima, koji se u mnogim mrežnim infrastrukturama često smatraju „baukom“. U ovom poglavlju pokušavamo da demistifikujemo kako oni funkcionišu i kako da implementirate besplatno izdavanje sertifikata u Linuxu za vašu organizaciju.

U Poglavlju 9, „RADIUS usluge za Linux“, objašnjeno je kako da koristite RADIUS u Linuxu kao autentifikaciju za različite mrežne uređaje i usluge.

U Poglavlju 10, „Usluge raspoređivača opterećenja za Linux“, objašnjeno je da je Linux odličan raspoređivač opterećenja, jer omogućava „besplatne“ usluge raspoređivanja opterećenja vezane za svako radno opterećenje, a ne tradicionalna, skupa i monolitna rešenja za raspoređivanje opterećenja „po centru podataka“, koja viđamo veoma često.

U Poglavlju 11, „Hvatanje i analiza paketa u Linuxu“, razmatramo korišćenje Linuxa kao hosta za hvatanje paketa. Ovo poglavlje se odnosi na način kako da to omogućimo na mreži, kao i na istraživanje različitih metoda filtriranja za dobijanje informacija koje su vam potrebne za rešavanje problema. Koristimo razne napade na VoIP sistem da bismo prikazali kako bi trebalo da obavimo ovaj posao.

Poglavlje 12, „Nadzor mreže pomoću Linuxa“, odnosi se na korišćenje Linuxa za centralno evidentiranje saobraćaja pomoću sysloga, kao i na upozorenja u realnom vremenu o ključnim rečima pronađenim u evidencijama. Takođe razmatramo obrasce za evidentiranje toka mrežnog saobraćaja pomoću NetFlowa i povezanih protokola.

U Poglavlju 13, „Sistemi za sprečavanje upada u Linuxu“, objašnjeno je da se Linux aplikacije koriste za upozoravanje o uobičajenim napadima i za njihovo blokiranje, kao i za dodavanje važnih metapodataka informacijama o saobraćaju. Istražujemo dva različita rešenja u vezi sa tim i pokazujemo kako da primenite različite filtere da biste otkrili različite obrasce u saobraćaju i u napadima.

Poglavlje 14, „Honeypot usluge u Linuxu“, odnosi se na korišćenje honeypotova kao „hostova za prevaru“ za odvraćanje pažnje i kašnjenje napadača, pri čemu se braniocima obezbeđuju upozorenja velike tačnosti. Takođe će biti reči o korišćenju honeypotova za istraživanje trendova zlonamernog ponašanja na javnom Internetu.

Izvucite maksimum iz ove knjige

U ovoj knjizi ćemo se fokusirati na većinu naših primera i nadovezati na podrazumevanu instalaciju Ubuntu Linuxa. Svakako možete da instalirate

Ubuntu na „goli" hardver, ali ćete možda otkriti da korišćenje rešenja za virtuelizaciju, kao što su VMware (Workstation ili ESXi), VirtualBox ili Proxmox, može zaista koristiti vašem učenju (sve ovo je, osim VMware Workstationa, besplatno). Korišćenjem opcije virtuelizacije možete usput da pravite „snimke" vašeg hosta na poznatim dobrim tačkama, što znači da, ako nešto pokvarite dok eksperimentišete sa nekom alatkom ili funkcijom, veoma lako možete da potrete tu promenu i da pokušate ponovo.

Osim toga, upotreba virtuelizacije omogućava da napravite više kopija vašeg hosta kako biste mogli da implementirate funkcije ili usluge na logičan način, umesto da pokušavate da sve usluge koje razmatramo u ovoj knjizi stavite na isti host.

U ovoj knjizi koristimo nekoliko Linux servisa, uglavnom implementiranih na Ubuntu Linux verziji 20 (ili novijoj). Ove usluge su sažete ovde:

OS KOMPONENTE ILI SERVISI KOJI SU RAZMATRANI U OVOJ KNJIZI	GDE I KAKO SE KORISTE
Netcap, Nmap	alatke koje pomažu u rešavanju problema sa žičnom ili bežičnom mrežom; Nmp će se posebno pojavljivati u ovoj knjizi
Kismet, Wavemon, LinSSID	različite alatke za procenu bežične mreže
iptables i nftables	izvorne implementacije firewalla dostupne u Linuxu
SELinux i AppArmor	komplet alatki za zaštitu vašeg Linux hosta
Berkely Internet Name Domain (BND)	DNS server koji je izvorni za Linux i veoma je široko rasprostranjen; održava ga **Internet Systems Consortium (ISC)**
ISC DHCP	DHCP server koji se najčešće koristi u Linuxu; takođe ga održava ISC
OpenSSL	najčešće korišćena alatka za rad sa sertifikatima i za dijagnostikovanje problema sa sertifikatima; takođe ćemo je koristiti za primenu * servera za izdavanje sertifikata.
FreeRADIUS (Remote Authentication Dial-In User Service)	usluga autentifikacije koja se najčešće koristi za centralnu autentikaciju VPN-ova, bežične usluge ili bilo koji broj drugih usluga na mreži
HaProxy	rešenje za raspoređivanje opterećenja zasnovano na Linuxu koje omogućava da rasporedite radna opterećenja na više servera
Rsyslog	osnovni syslog server za Linux, koji omogućava da centralizujete evidencije sa svih vrsta hostova i uređaja

Osim toga, koristimo ili razmatramo nekoliko „dodatnih“ Linux alatki koje možda ne poznajete:

ALATKE KOJE SU RAZMATRANE U KNJIZI	KAKO I KADA SE KORISTE
tcpdump, Wireshark, TShark	različite alatke za hvatanje paketa
dSniff, Ettercap, Bettercap	alatke koje se mogu zlonamerno koristiti za hvatanje paketa, posebno onih sa podacima koje će vaš napadač smatrati zanimljivim (kao što su akreditivi)
NetworkMiner	alatka za pomeranje kroz velike pakete da bi bili prikupljeni podaci od interesa
DShield projekat	analiza evidencije zasnovane na Internetu koja će vam pomoći da pratite trendove internet saobraćaja, kako na vašem firewallu, tako i na Internetu
snmpget, snmpwalk	alatke komandne linije za prikupljanje SNMP informacija
LibreNMS	**Network Managament System (NMS)** koji možete brzo i lako da primenite za male i srednje organizacije; u ovoj knjizi ćemo koristiti *unapred izgrađenu virtuelnu mašinu LibreNMS, mada je svakako možete instalirati „od nule“ ako želite
nfcapd, nfdump	alatke komandne linije za snimanje i prikaz ili filtriranje *NetFlow podataka.
NfSen	jednostavan frontend zasnovan na Vebu na vrhu nfcapda i nfdumpa
Suricata i Snort	dva **popularna sistema za sprečavanje upada (IPS–Intrusion Protection Systems)**; u ovoj knjizi se fokusiramo na Suricatu i koristimo unapred spakovane distribucije SELKS i Security Onion
Zeek	alatka za dodavanje različitih metapodataka mrežnom saobraćaju, koja vam štedi vreme i trud koje biste uložili kada biste to radili ručno. Na primer, koji CA je izdao sertifikat ili u kojoj zemlji se nalazi ta napadačka IP adresa? U ovoj knjizi koristimo Zeek instalaciju, koja se nalazi u distribuciji Security Onion.
Portsproof	honeypot zasnovan na portovima, koji možete da koristite za osnovne pristupe prevare protiv napadača
Cowrie	Telnet i SSH honeypot, koji prate akreditive koje napadači koriste, kao i razne komande koje isprobavaju tokom svojih napada
WebLabyrinth	veb honeypot koji napadačima nudi beskonačan broj veb stranica; ovakve alatke su posebno dobre u usporavanju ili „betoniranju“ napadačevih automatizovanih alatki za skeniranje

ALATKE KOJE SU RAZMATRANE U KNJIZI	KAKO I KADA SE KORISTE
Thinkst Canary	komercijalno rešenje koje se može maskirati u razne vrste infrastrukture
Internet Storm Center honeypot projekat	SSH i telnet honeypot zasnovani na Internetu sa centralnom konfiguracijom i izveštavanjem; ovo omogućava da učestvujete u istraživačkom projektu širom Interneta, koji prati trendove u metodima napadača

Većinu navedenih alatki i usluga možete da instalirate na jednom Linux hostu dok budete čitali naredna poglavlja. Ovo dobro funkcioniše za laboratorijsko podešavanje, ali na pravoj mreži ćete, naravno, podeliti važne servere na različite hostove.

Neke alatke istražujemo kao deo unapred izgrađene ili unapred spakovane distribucije. U ovim slučajevima svakako možete da instalirate ovu istu distribuciju u vaš hipervizor, ali takođe je možete pratiti u određenom poglavlju da biste dobro procenili koncepte, pristupe i nedostatke onako kako su prikazani.

Preuzimanje kolornih slika

Takođe smo pripremili PDF datoteku, koja sadrži kolorne slike ekrana/dijagrama upotrebljenih u knjizi. Možete da preuzmete ovu datoteku sa adrese:

https://bit.ly/3z8DF9x

Preuzimanje datoteka sa primerima koda

Možete da preuzmete datoteke sa primerima koda za ovu knjigu sa GitHuba https://bit.ly/3Hp3uW1

Možete izvršiti ažuriranje koda ako ono postoji u postojećem GitHub spremištu.

Upotrebljene konvencije

Postoji veliki broj konvencija teksta koje su upotrebljene u ovoj knjizi.

`Code InText` - Ukazuje na reči koda u tekstu, nazive tabela baze podataka, nazive direktorijuma, nazive datoteka, ekstenzije datoteka, nazive putanja, skraćene URL-ove, korisnički unos i Twitter postove. Evo i primera: „Sve tri alatke su besplatne i možete da ih instalirate pomoću standardne komande `apt-get install <package name>`.“

Blok koda je prikazan na sledeći način:

```
$ sudo kismet –c <wireless interface name>
```

Podebljana slova - Ukazuju na novi termin, važnu reč ili reči koje vidite na ekranu. Na primer, reči u menijima ili okvirima za dijalog prikazane su u tekstu podebljanim slovima. Evo i primera: „U Linux GUI-u prvo kliknite na ikonu mreže na gornjoj tabli, a zatim izaberite **Settings** za vaš interfejs."

Stupite u kontakt

Povratne informacije od naših čitalaca su uvek dobrodošle.

Opšte povratne informacije - Ako imate pitanja o bilo kom aspektu ove knjige, pošaljite nam e-mail, sa navedenim naslovom knjige u temi vaše poruke na adresu customercare@packtpub.com.

Štamparske greške - Iako smo preduzeli sve mere da bismo obezbedili tačnost sadržaja, greške su moguće. Ako pronađete neku grešku u ovoj knjizi, bili bismo zahvalni ako biste nam to prijavili. Posetite veb stranu knjige na našem sajtu:

https://bit.ly/3FDiD5z i ostavite komentar.

Piraterija - Ako pronađete ilegalnu kopiju naše knjige u bilo kojoj formi na Internetu, molimo vas da nas o tome obavestite i da nam pošaljete adresu lokacije ili naziv veb sajta. Kontaktirajte sa nama na adresi copyright@packt.com ili kombib@gmail.com pošaljite nam link ka sumnjivom materijalu.

Ako ste zainteresovani da postanete autor - Ako postoji tema za koju ste specijalizovani, a zainteresovani ste da pišete ili sarađujete na nekoj od knjiga, pogledajte vodič za autore na adresi authors.packtpub.com.

Podelite svoje mišljenje

Želimo da saznamo vaše mišljenje nakon što pročitate „Linux za profesionalce umrežavanja". Direktno pristupite stranici Amazon review za ovu knjigu i napišite vaše povratne informacije.

Vaša recenzija je važna za nas i tehničku zajednicu i pomoći će nam da proverimo kakav je kvalitet sadržaja koji isporučujemo.

DEO I

Osnove Linuxa

U ovom delu su opisane različite Linux opcije dostupne čitaocima i opisano je zašto bi možda trebalo da izaberu Linux za isporuku različitih mrežnih funkcija ili usluga. Osim toga, razmotrena je detaljno osnovna Linux mrežna konfiguracija. U ovom delu je pripremljen „teren" za sva naredna poglavlja.

Ovaj deo knjige se sastoji od dva poglavlja:

- **Poglavlje 1**, „Dobrodošli u Linux porodicu!"
- **Poglavlje 2**, „Osnovna Linux mrežna konfiguracija i operacije – korišćenje lokalnih interfejsa"



1

Dobrodošli u Linux porodicu!

U ovoj knjizi istražujemo Linux platformu i različite operativne sisteme zasnovane na Linuxu – posebno kako Linux može dobro da funkcioniše za mrežne usluge. Pre nego što pogledamo osnovnu konfiguraciju i rešavanje problema ovog operativnog sistema, prvo ćemo razmotriti njegovu istoriju. Potom ćemo se posvetiti izradi različitih mrežnih usluga u Linuxu koje često možete da vidite u većini organizacija. Dok budemo napredovali, izradićemo prave usluge na pravim hostovima, sa naglaskom na zaštiti i rešavanju problema svake usluge. Na kraju bi trebalo da dovoljno poznajete svaku od ovih usluga da biste počeli da implementirate neke od njih ili sve u svojoj organizaciji. Pošto *svako putovanje počinje jednim korakom*, napravićemo taj korak i počećemo opšte razmatranje Linux platforme.

U ovom poglavlju ćemo započeti naše „putovanje“ istraživanjem Linuxa kao porodice operativnih sistema. Svi ti operativni sistemi su povezani, ali svaki je jedinstven na svoj način, sa različitim snagama i funkcijama.

Razmotrićemo sledeće teme:

- zašto je Linux dobar za tim umrežavanja
- Mainstream data center Linux
- specijalne Linux distribucije
- virtuelizacija
- odabir Linux distribucije za vašu organizaciju

Zašto je Linux dobar za tim umrežavanja

U ovoj knjizi ćemo istražiti kako da podržimo i rešimo probleme sa svojom mrežom korišćenjem Linuxa i Linux alatki i kako da bezbedno primenimo zajedničku mrežnu infrastrukturu na Linux platformama.

Zašto biste želeli da koristite Linux za ove svrhe? Za početak, arhitektura, istorija i kultura Linuxa usmeravaju administratore ka skriptovanju i automatizaciji procesa. Dok dovođenje toga do krajnosti može „uvaliti" ljude u smešne situacije, rutinski zadaci skriptovanja mogu zaista da uštede vreme.

U stvari, skriptovanje zadataka koji nisu rutinski, kao što je nešto što treba da se uradi jednom godišnje, takođe može da bude spasonosno – to znači da administratori ne moraju ponovo da uče kako da rade ono što su radili pre 12 meseci.

Skriptovanje rutinskih zadataka je još veća pobeda. Tokom mnogo godina su Windows administratori shvatili da obavljanje jednog zadatka stotinu puta u **grafičkom korisničkom interfejsu (GUI - Graphical User Interface)** garantuje da će pogrešno kliknuti bar nekoliko puta. Sa druge strane, ovo skriptovanje zadataka garantuje konzistentne rezultate. I ne samo to, već na mreži na kojoj administratori rutinski obavljaju operacije za stotine ili hiljade stanica skriptovanje je često jedini način izvršavanja većeg broja zadataka.

Drugi razlog zbog kojeg administratori mreže preferiraju Linux platforme je činjenica da Linux (a pre toga, Unix) postoji otkako postoje mreže čiji je on deo. Na strani servera Linux (ili Unix) usluge su ono što ih je definisalo, gde su odgovarajuće Windows usluge kopije koje su se tokom vremena uglavnom povećale toliko da imaju paritetne funkcije.

Na strani radne stanice, ako vam je potrebna alatka za administriranje ili dijagnostikovanje nečega na vašoj mreži, verovatno je već instalirana. Ako alatka koju tražite nije instalirana, to je komanda u jednom redu koju možete da instalirate i pokrenete, zajedno sa svim drugim potrebnim alatkama, bibliotekama ili zavisnostima. A dodavanje te alatke ne zahteva plaćanje licence – i Linux i sve alatke instalirane u Linuxu su (skoro bez izuzetka) besplatne i otvorenog koda.

Na kraju, i na strani servera i na strani desktopa, istorijski gledano, Linux je bio besplatan. Čak i sada, kada profitne kompanije naplaćuju licence za neke od glavnih podržanih distribucija (na primer, za Red Hat i SUSE), one nude besplatne verzije tih distribucija. Red Hat nudi Fedora Linux i CentOS, koji su besplatni i, u određenoj meri, ponašaju se kao probne verzije za nove funkcije u Red Hat Enterprise Linuxu. SUSE Linux (naplaćuje se) i OpenSUSE (besplatno) su takođe veoma slični, pri čemu je distribucija SUSE rigoroznije testirana i verzije se redovnije nadgrađuju. Verzije za preduzeća su, obično, licencirane na ograničeno vreme, pri čemu ta licenca omogućava korisniku pristup tehničkoj podršci i, u mnogim slučajevima, ažuriranjima OS-a.

Mnoge kompanije se odlučuju za licencirane verzije operativnog sistema **spremne za preduzeća (enterprise-ready)**, dok mnoge druge odlučuju da izgrade svoje infrastrukture na besplatnim verzijama OpenSUSE-a, CentOS-a ili Ubuntua. Dostupnost besplatnih verzija Linuxa znači da mnoge organizacije mogu da rade sa znatno nižim IT troškovima, što je u velikoj meri uticalo na to gde je dospela softverska industrija.

Zašto je Linux važan?

Jedna od šala u zajednici informacionih tehnologija je da će sledeća godina uvek biti *godina Linux desktopa* – u kojoj ćemo svi prestati da plaćamo licence za desktop računare i poslovne aplikacije, a sve će da bude besplatno i otvorenog koda.

Umesto toga, dogodilo se da Linux kontinuirano prodire u serversku i infrastrukturnu stranu mnogih okruženja.

Linux je postao oslonac u većini centara podataka, čak i ako te organizacije sebe smatraju okruženjem *samo za Windows*. Mnoge infrastrukturne komponente pokreću Linux ispod „pokrivača“, sa lepim veb frontendom koji ga pretvara u rešenje za dobavljače. Ako imate **mrežu za čuvanje podataka (StorageArea Network - SAN)**, ona verovatno pokreće Linux, kao što to rade i vaši **raspoređivači opterećenja**, **pristupne tačke** i **bežični kontroleri**. Mnogi **ruteri** i **svičevi** pokreću Linux, kao i skoro sva nova rešenja za *softverski definisano umrežavanje.*

Skoro bez greške, proizvodi za bezbednost informacija zasnovani su na Linuxu. Tradicionalni firewallovi i firewallovi *sledeće generacije*, **sistemi za otkrivanje i sprečavanje upada (IDS/IPS)**, **sistemi za upravljanje bezbednosnim informacijama i događajima (Security Information and Event Management - SIEM)** i serveri za evidentiranje su zasnovani na Linuxu. Zašto je Linux toliko rasprostranjen? Postoji mnogo razloga:

- To je zreo operativni sistem.

- Ima integrisani sistem „zakrpa“ i ažuriranja.
- Osnovne funkcije su jednostavne za konfigurisanje. Međutim, složenije funkcije operativnog sistema mogu da budu teže za konfigurisanje nego u Windowsu (za više informacija pogledajte poglavlje o DNS-u ili DHCP-u).
- Sa druge strane, mnoge funkcije koje bi mogle da budu *na prodaju* u Windows okruženju možete besplatno da instalirate u Linuxu.
- Pošto je Linux skoro u potpunosti zasnovan na datotekama, prilično lako možete da ga zadržite na poznatoj osnovi ako ste dobavljač koji svoj proizvod zasniva na njemu.
- Možete da napravite skoro sve na Linuxu, s obzirom na pravu kombinaciju besplatnih paketa i paketa otvorenog koda, nekih skriptova, a možda i nekog prilagođenog kodiranja.
- Ako izaberete odgovarajuću distribuciju, sam OS je besplatan, što je odličan motiv za dobavljača koji pokušava da poveća profit ili za kupca koji pokušava da snizi svoje troškove.

Ako vas privlači novi pokret **Infrastructure as Code**, onda ćete otkriti da je skoro svaki jezik kodiranja zastupljen u Linuxu i da se aktivno razvija – od novih jezika, kao što su **Go** i **Rust**, pa sve do **Fortrana** i **Cobola**. Čak su i **PowerShell** i **.NET**, koji su nastali iz Windowsa, potpuno podržani u Linuxu. Većina infrastrukturnih mehanizama za orkestraciju (na primer, **Ansible**, **Puppet** i **Terraform**) prvo su pokrenuti i podržani u Linuxu.

Na strani „oblaka“ današnje IT infrastrukture činjenica da je Linux besplatan dovela je do toga da dobavljači usluga u „oblaku“ guraju svoje klijente ka tom kraju spektra skoro od samog početka. Ako ste se pretplatili na bilo koju uslugu u „oblaku“ koja je opisana kao *serverless* ili *as a Service* u pozadini, verovatno se to rešenje sastoji skoro od celog Linuxa.

Pošto ste videli da se serverska i infrastrukturna strana IT-a pomeraju ka Linuxu, treba da imate na umu da današnji mobilni telefoni stalno postaju najveća *desktop* platforma u današnjoj računarskoj stvarnosti. U današnjem svetu mobilni telefoni su, uglavnom, zasnovani na iOS-u ili Androidu, a oba su (verovatno ste pogodili) zasnovana na Unixu/Linuxu! Dakle, *godina Linux desktopa* nam se prikrala, zahvaljujući promeni definicije desktopa.

Sve ovo čini Linux veoma važnim za današnje profesionalce za umrežavanje ili IT. U ovoj knjizi se fokusiramo na korišćenje Linuxa kao desktop okvira sa alatkama za profesionalce umrežavanja, kao i na bezbedno konfigurisanje i isporuku različitih mrežnih usluga na Linux platformi.

Istorija Linuxa

Da bismo razumeli poreklo Linuxa, moramo da znamo poreklo Unixa. Unix je razvijen kasnih šezdesetih i ranih sedamdesetih godina prošlog veka u „Bell Labsu". Dennis Ritchie i KenThompson su bili glavni programeri Unixa. Naziv Unix je zapravo bila igra reči zasnovana na nazivu **Multics**, ranijem operativnom sistemu kojim su inspirisane mnoge Unixove funkcije.

Richard Stallman i Free Software Foundation su 1983. godine pokrenuli projekat GNU (rekurzivni akronim – **GNU's Not Unix**) u kojem su težili da kreiraju operativni sistem sličan Unixu, a dostupan svima besplatno. Iz njihovog uloženog truda proizašao je *GNU Hurdkernel*, koji bi većina smatrala prethodnikom današnjih verzija Linuxa (SFS bi više voleo da ih sve zovemo GNU/Linux).

Linus Torvalds je 1992. godine objavio Linux, prvi potpuno realizovan GNU kernel. Važno je napomenuti da se mainstream Linux obično smatra jezgrom koje može da se koristi za kreiranje operativnog sistema, a ne operativnim sistemom. Linux se još uvek održava, sa Linusom Torvaldsom kao vodećim programerom, ali danas postoji mnogo veći tim pojedinaca i korporacija u svojstvu saradnika. Dakle, dok se Linux tehnički odnosi samo na jezgro, u softverskoj industriji se generalno odnosi na bilo koji operativni sistem koji je izgrađen na tom kernelu.

Od sedamdesetih godina prošlog veka, objavljene su stotine zasebnih verzija Linuxa, koje se, obično, nazivaju **distribucija** (ili, skraćeno, **distro**). Svaka distribucija je zasnovana na Linux kernelu iz tog vremena, zajedno sa infrastrukturom za instalaciju i sistemom spremišta za OS i za ažuriranja. Većina je na neki način jedinstvena kada je reč o kombinaciji osnovnih paketa ili fokusu distribucije – neke su možda suviše male da bi se uklopile u manje hardverske platforme, neke se možda fokusiraju na bezbednost, neke su možda namenjene kao *workhorse* operativni sistem opšte namene za preduzeća i tako dalje.

Neke distribucije su bile „mejnstrim" neko vreme, a nekima je opadala popularnost kako je vreme prolazilo. Ono što sve distribucije dele je Linux jezgro na kojem su izgrađene za kreiranje svojih distribucija. Mnoge distribucije su zasnovale svoj operativni sistem na drugoj distribuciji, prilagođavajući je dovoljno da bi opravdale što su nazvale svoje implementacije novom distribucijom. Ovaj trend nam je dao ideju o „Linux porodičnom stablu" – na kojem desetine distribucija mogu da „rastu" iz zajedničkog „korena". To je istraženo na DistroWatch veb sajtu https://distrowatch.com/dwres.php?resource=family-tree.

Alternativa Linuxu, posebno u Intel/AMD/ARM hardverskom prostoru, je **Berkeley Software Distribution (BSD)** Unix. BSD Unix je potomak originalnog **Bell Labs Unixa** i uopšte nije zasnovan na Linuxu. Međutim, BSD i mnogi njegovi derivati su i dalje besplatni i imaju mnoge karakteristike (i dosta koda) kao u Linuxu.

Do danas, naglasak i Linuxa i BSD Unixa je na to da su oba besplatno dostupni operativni sistemi. Skoro sve te komercijalne verzije imaju odgovarajuće besplatne verzije.

U ovom odeljku pregledali smo istoriju i značaj Linuxa u računarskom svetu. Shvatili ste kako je nastao Linux i kako je postao popularan u određenim delovima računarskog „pejzaža". Sada ćemo početi da razmatramo različite verzije Linuxa koje su nam dostupne. To će nam pomoći da se nadovežemo na informacije koje su nam potrebne da bismo mogli da izaberemo distribuciju koju ćemo koristiti kasnije u ovom poglavlju.

Mainstream data center Linux

Kao što smo već napomenuli, Linux nije monolitna „stvar", već pre raznolik ili čak podeljen eko-sistem različitih distribucija. Sve Linux distribucije su zasnovane na istom GNU/Linux kernelu, ali su upakovane u grupe sa različitim ciljevima i filozofijama, pa organizacije mogu da iz različitog spektra izaberu distribuciju kada žele da počnu standardizaciju na svojim platformama servera i radnih stanica.

Glavne distribucije koje obično viđamo u savremenim centrima podataka su **Red Hat**, **SUSE** i **Ubuntu**, pri čemu je **FreeBSD Unix** još jedna alternativa (iako sada mnogo manje popularna nego u prošlosti). To ne znači da se druge distribucije ne pojavljuju na desktopu ili u centrima podataka, ali ovo su one koje ćete najčešće viđati. Sve one imaju i desktop i serversku verziju – serverske verzije su često „skraćene", sa svojom poslovnom produktivnošću, medijskim alatkama i, često, uklonjenim GUI-em.

Red Hat

Red Hat je nedavno kupio IBM (2019. godine), ali i dalje održava Fedoru kao jedan od svojih glavnih projekata. Fedora ima i serversku i desktop verziju i ostaje besplatno dostupna. Komercijalna verzija Fedore je **Red Hat Enterprise Linux (RHEL)**. RHEL je komercijalno licenciran i ima formalni kanal podrške.

CentOS je prvo bio besplatna verzija Linuxa koju podržava zajednica, a bio je funkcionalno kompatibilan sa verzijom Red Hat Enterprisea. To ga je učinilo veoma popularnim za implementacije servera u mnogim organizacijama. U januaru 2014. godine Red Hat je uzeo CentOS pod svoje okrilje, postavši formalni sponzor distribucije. Krajem 2020. godine objavljeno je da CentOS više neće biti održavan kao RHEL kompatibilna distribucija, već će se, umesto toga, „uklopiti" negde između Fedore i RHEL-a – ne toliko nov da bi bio „najnapredniji", ali ni toliko stabilan kao RHEL. Kao deo ove promene, CentOS je preimenovan u **CentOS Stream**.

Konačno, Fedora je distribucija koja ima najnovije funkcije i kod i u kojoj se nove funkcije isprobavaju i testiraju. CentOS Stream distribucija je stabilnija, ali je i dalje „ispred“ RHEL-a. RHEL je stabilan, potpuno testiran operativni sistem, sa formalnom podrškom.

Oracle/Scientific LinuX

Oracle/Scientific LinuX se takođe može videti u mnogim centrima podataka (i u „Oracleovoj“ ponudi u „oblaku“). Oracle Linux je zasnovan na Red Hatu, a potpuno je kompatibilan sa RHEL-om. Oracle Linux je besplatan za preuzimanje i korišćenje, ali podrška „Oraclea“ je zasnovana na pretplati.

SUSE

OpenSUSE je distribucija zajednice na kojoj je zasnovan SUSE Linux, slično kao što je RedHat Enterprise Linux zasnovan na Fedori.

SUSE Linux Enterprise Server (obično nazivan **SLES**) je u ranijim danima Linuxa bio, uglavnom, evropski konkurent za Red Hat distribuciju, sa sedištem u SAD. Ti dani su, međutim, prošlost, a SUSE Linux se (skoro) može naći i u Indijani i u Italiji u modernim centrima podataka.

Slično vezi između RedHata i CentOS-a, SUSE održava i desktop i serversku verziju. Pored toga, održava verziju operativnog sistema „visokih performansi“, koja se isporučuje sa optimizacijama i alatkama unapred instaliranim za paralelno računarstvo. OpenSUSE zauzima „uzlaznu“ poziciju u odnosu na SLES, pa promene mogu da se uvedu u distribuciju malo lakšu za promene koje možda neće uvek uspeti iz prvog pokušaja. OpenSUSE Tumbleweed distribucija ima najnovije funkcije i verzije, pa je OpenSUSE Leap bliži kada je reč o verzijama i stabilnosti SLE verzijama operativnog sistema. Nije slučajno što je ovaj model sličan RedHat porodici distribucija.

Ubuntu

Ubuntu Linux održava Canonical - besplatan je za preuzimanje, bez posebnih komercijalnih ili „uzlaznih“ opcija. Zasnovan je na Debianu i ima jedinstven ciklus objavljivanja. Nove serverske i desktop verzije se objavljuju na svakih šest meseci. Verzija **Long-Term Support (LTS)** se objavljuje svake druge godine, sa podrškom za LTS verzije i servera i desktopa koje su pokrenute pet godina od datuma objavljivanja. Kao i kod drugih većih „igrača“, podrška je zasnovana na pretplati, iako je besplatna podrška zajednice, takođe, održiva opcija.

Kao što i pretpostavljate, serverska verzija Ubuntua je više fokusirana na osnovne operativne sisteme, mrežu i usluge centra podataka. Izbor GUI-a je često opozvan tokom instalacije serverske verzije. Međutim, Desktop verzija ima nekoliko instaliranih paketa za kancelarijsku produktivnost, kreiranje medija i konverziju, kao i neke jednostavne igre.

BSD/FreeBSD/OpenBSD

Kao što smo ranije napomenuli, BSD „stablo" porodice je izvedeno iz Unixa, a ne iz Linux kernela, ali postoji mnogo zajedničkog koda, posebno u paketima koji nisu deo kernela.

FreeBSD i OpenBSD su istorijski smatrani „bezbednijim" od ranijih verzija Linuxa. Zbog toga su mnogi firewallovi i mrežni uređaji napravljeni na osnovu BSD OS porodice i ostali su na ovom OS-u do danas. Jedna od „vidljivijih" BSD varijanti je Appleov komercijalni operativni sistem **OS X** (sada **macOS**). Ovo je zasnovano na Darwinu, koji je, zauzvrat, grana BSD-a.

Međutim, kako je vreme odmicalo, Linux je narastao tako da ima većinu istih bezbednosnih mogućnosti kao BSD, sve dok BSD možda nije imao bezbednije podrazumevane postavke od većine Linux alternativa.

Linux sada ima dostupne bezbednosne module koji značajno povećavaju njegov bezbednosni položaj. **SELinux** i **AppArmor** su dve glavne opcije koje su dostupne. SELinux je „izrastao" iz Red Hat distribucija i u potpunosti je implementiran i za SUSE, Debian i Ubuntu. AppArmor se, obično, smatra opcijom koja je jednostavnija za implementaciju, sa mnogim (ali ne svim) istim funkcijama. AppArmor je dostupan na Ubuntuu, SUSE-u i većini drugih distribucija (sa izuzetkom RHEL-a). Obe opcije koriste pristup zasnovan na smernicama kako bi značajno povećale ukupan bezbednosni položaj OS-a na kojem su instalirane.

Nakon što je Linux evoluirao, tako što se više fokusirao na bezbednost, posebno sa SELinuxom ili AppArmorom koji su dostupni (i preporučeni) za većinu modernih Linux distribucija, „bezbedniji" argument BSD-a u odnosu na Linux je sada uglavnom istorijska percepcija, a ne činjenica.

Specijalne Linux distribucije

Izuzev mainstream Linux distribucija, postoji nekoliko distribucija koje su namenski napravljene za određeni skup zahteva. Sve su izgrađene na više mainstream distribucija, ali su prilagođene tako da odgovaraju specifičnim potrebama. Ovde ćemo opisati nekoliko distribucija koje ćete najverovatnije videti ili koristiti kao profesionalac umrežavanja.

Većina komercijalnih dobavljača **Network-attached Storage (NAS)** i SAN zasniva se na Linuxu ili BSD-u. U vreme pisanja ovog teksta čini se da su lideri u NAS/SAN uslugama otvorenog koda **TrueNAS** (ranije **FreeNAS**) i **XigmaNAS** (ranije **NAS4Free**). Oba imaju besplatne i komercijalne ponude.

Firewallovi otvorenog koda

Kompanije za umrežavanje i bezbednost nude širok izbor firewallova, od kojih je većina zasnovana na Linuxu ili BSD-u. Mnoge kompanije nude besplatne firewallove, a neki od popularnijih su **pfSense** (dostupni su besplatne verzije i unapred izrađena hardverska rešenja), **OPNsense** (besplatno dostupan, uz donacije) i **Untangle** (koji takođe ima komercijalnu verziju). **Smoothwall** je još jedna alternativa, sa dostupnim besplatnim i komercijalnim verzijama.

U ovoj knjizi ćemo istražiti korišćenje ugrađenog firewalla u Linuxu za zaštitu pojedinačnih servera ili za zaštitu mrežnog perimetra.

Kali Linux

Potekao od **BackTrack-a**, a pre toga **KNOPPIX-a**, Kali Linux je distribucija zasnovana na Debianu koja je fokusirana na bezbednost informacija. Osnovna namena ove distribucije je da se prikupi što više korisnih alatki za testiranje prodiranja i etičkih hakerskih alatki na jednoj platformi, a zatim da se osigura da sve rade bez međusobnog ometanja. Novije verzije distribucije su fokusirane na održavanje interoperabilnosti ove alatke tokom ažuriranja OS-a i alatki (korišćenjem skupa alatki `apt`).

SIFT

SIFT je distribucija čiji je autor forenzički tim Instituta SANS, fokusirana na digitalnu forenziku i alatke za reagovanje na incidente i istrage. Slično kao i Kali, cilj SIFT-a je da je „sve na jednom mestu" za besplatne alatke/alatke otvorenog koda u jednoj oblasti – **Digital Forensicsand Incident Response (DFIR)**. Istorijski gledano, ovo je bila distribucija zasnovana na Ubuntuu, ali poslednjih godina to se promenilo – SIFT se sada distribuira i kao skript koji instalira alatke na Ubuntu desktopu ili Windows Services za Linux (koji se zasniva na Ubuntuu).

Security Onion

Security Onion je takođe sličan Kali Linuxu po tome što sadrži nekoliko alatki za bezbednost informacija, ali on se više fokusira sa pozicije branioca. Ova distribucija je usredsređena na lov na pretnje, nadzor bezbednosti mreže i upravljanje evidencijama. Neke od alatki u ovoj distribuciji su Suricata, Zeek i Wazuh.

Virtuelizacija

Virtuelizacija je odigrala veliku ulogu u usvajanju Linuxa i u omogućavanju rada sa više distribucija odjednom. Korišćenjem lokalnog hipervizora profesionalac umrežavanja može da pokrene desetine različitih „mašina“ na svom laptopu ili desktop računaru. VMware je bio pionir u ovom svetu (desktop i namenska virtuelizacija), a u međuvremenu su su im se pridružili Xen, KVM, VirtualBox, QEMU i mnogi drugi. Dok su VMware komercijalni proizvodi (osim VMware Playera), ostala navedena rešenja su, u vreme pisanja ove knjige, još uvek besplatna. VMwareov vodeći hipervizor ESXi takođe je dostupan besplatno kao samostalan proizvod.

Linux i računarstvo u „oblaku“

Sve veća stabilnost Linuxa i činjenica da je virtuelizacija sada mejnstrim na mnogo načina su omogućili naše moderne eko-sisteme u „oblaku“. Dodajmo tome sve veće mogućnosti automatizacije u postavljanju i održavanju backend infrastrukture i sofisticiranost koja je dostupna programerima veb aplikacija i **interfejsima za programiranje aplikacija (API-ima)** i ono što dobijamo su današnje infrastrukture u „oblaku“. Ovo su neke od ključnih funkcija računarstva u „oblaku“:

- infrastruktura sa više zakupaca, u kojoj svaki korisnik održava svoje instance (virtuelne servere i virtuelne centre podataka) u „oblaku“
- granularni obračun troškova po mesecima ili, češće, po resursima koji se koriste tokom vremena
- pouzdanost koja je dobra ili bolja od pouzdanosti u mnogim savremenim centrima podataka (iako su nedavni prekidi u radu pokazali šta se dešava kada stavimo previše jaja u istu korpu)
- API-i koji čine automatizaciju infrastrukture relativno lakom, tj. toliko lakom da je za mnoge kompanije obezbeđivanje i održavanje njihove infrastrukture postala aktivnost kodiranja (često se naziva **Infrastructure as Code**)
- Ovi API-i omogućavaju povećanje (ili smanjenje) kapaciteta po potrebi, bilo da je reč o skladištu, izračunavanju, memoriji ili broju sesija.

Međutim, usluge u „oblaku“ posluju radi profita – svaka kompanija koja je odlučila da „prenese“ svoj centar podataka u uslugu u „oblaku“ verovatno je otkrila da se svi ti niski troškovi sabiraju tokom vremena, pa na kraju dostižu ili premašuju troškove njihovog lokalnog centra podataka. I dalje je često privlačnost na strani dolara, pošto se ti dolari troše na operativne troškove koji se mogu lakše pripisati direktno nego lokalni model kapitalnih izdataka (koji se obično naziva Cap-Ex, u poređenju sa Op-Ex modelima).

Kao što vidite, premeštanje centra podataka u uslugu u „oblaku“ donosi mnogo prednosti organizaciji koja verovatno ne bi imala tu opciju u lokalnom modelu. To postaje očiglednije kada koristite više funkcija samo za „oblak“.

Odabir Linux distribucije za vašu organizaciju

U mnogim slučajevima nije važna distribucija koju izaberete za svoj centar podataka – sve glavne distribucije imaju slične funkcije, često imaju identične komponente i često imaju slične opcije podrške dobavljača ili zajednice. Međutim, zbog razlika između ovih distribucija, važno je da izaberete jednu distribuciju (ili skup sličnih).

Željeni ishod je da vaša organizacija standardizuje jednu distribuciju pomoću koje vaš tim može da razvije svoju stručnost. To takođe znači da možete da radite sa istim timom za eskalaciju za napredniju podršku i rešavanje problema, bilo da je reč o konsultantskoj organizaciji, plaćenom timu za podršku dobavljačima ili grupi istomišljenika na raznim internet forumima. Mnoge organizacije kupuju ugovore o podršci sa jednom od kompanija iz „velike trojke“ („Red Hat“, SUSE ili „Canonical“, u zavisnosti od njihove distribucije).

Verovatno ne biste želeli da budete u sledećoj situaciji u kojoj se našlo nekoliko klijenata. Nakon što su unajmili osobu koja je voljna da uči, godinu dana kasnije, ti klijenti su otkrili da je svaki od servera koji su izrađeni te godine bio na različitoj distribuciji Linuxa, od kojih je svaka napravljena malo drugačije. Ovo je kratak put do toga da vaša infrastruktura postane čuveni „naučni eksperiment“ koji se nikada ne završava!

Uporedite tu situaciju sa situacijom drugog klijenta – njegov prvi server je bio **SUSE Linuxfor SAP**, koji je, kao što sam naziv govori, SUSE Linux server, spakovan sa SAP aplikacijom koju je klijent kupio (SAP HANA). Kako je njegov Linux otisak rastao zbog više usluga, ostao je na SUSE platformi, ali je na kraju imao „pravu“ SLES distribuciju. Ovo ga je održalo na jednom operativnom sistemu i, što je za njega podjednako važno, na jednoj licenci za podršku sa SUSE-om. Mogao je da svoju obuku i stručnost usmeri na SUSE. Još jedna ključna prednost za njega bila je što je, kako je dodavao više servera, mogao da primeni jedan „tok“ ažuriranja i „zakrpa“ sa pristupom u fazama. U svakom ciklusu „zakrpe“ prvo su „zakrpljeni“ manje važni serveri, a serveri osnovnih poslovnih aplikacija su „zakrpljeni“ nekoliko dana kasnije nakon što je testiranje završeno.

Pri odabiru distribucije treba da izaberete jednu od većih. Ako ljudi u vašem timu odobravaju upotrebu jedne od tih distribucija, onda to svakako uzmite u obzir. Verovatno ćete želeti da ostanete prilično blizu jedne od mainstream distribucija kako biste mogli da je koristite u svojoj organizaciji, tj. blizu nečega što se redovno održava i ima model plaćene pretplate koji je dostupan za podršku – čak i ako smatrate da vam nije potrebna plaćena podrška, danas to možda nije uvek slučaj.

Zaključak

Sada, kada smo razmotrili istoriju Linuxa, zajedno sa nekoliko glavnih distribucija, nadam se da ćete bolje da cenite istoriju i centralni značaj operativnih sistema u našem društvu. Posebno se nadam da imate neke dobre kriterijume koji će vam pomoći da izaberete distribuciju za vašu infrastrukturu.

U ovoj knjizi ćemo izabrati Ubuntu kao našu distribuciju. To je besplatna distribucija, koja u svojoj LTS verziji ima OS u čiju podršku se možemo pouzdati dok radimo na različitim scenarijama, verzijama i primerima o kojima će biti reči. To je takođe distribucija koja je izvorna za Windows (u Windows uslugama za Linux). Ovo je čini lakom distribucijom za upoznavanje, čak i ako nemate rezervni hardver servera, radne stanice, niti platformu za virtuelizaciju za testiranje.

U sledećem poglavlju ćemo razmotriti postavljanje Linux servera ili radne stanice na mrežu. Prikazaćemo korišćenje lokalnih interfejsa i dodavanje IP adresa, maske podmreže i sve rute koje su potrebne da bi Linux host radio na novoj ili postojećoj mreži.

Pročitajte još

- Red Hat Linux: https://www.redhat.com/en
- Fedora: https://getfedora.org/
- CentOS: https://www.centos.org/
- SUSE Linux: https://www.suse.com/
- OpenSUSE: https://www.opensuse.org/
- Ubuntu Linux: https://ubuntu.com/
- Windows Subsystem for Linux: https://docs.microsoft.com/en-us/ https://docs.microsoft.com/en-us/windows/wsl/about
- FreeBSD Unix: https://www.freebsd.org/
- OpenBSD Unix: https://www.openbsd.org/

- Linux/BSD differences: https://www.howtogeek.com/190773/htg-explains-whats-the-difference-between-linux-and-bsd/
- TrueNAS: https://www.truenas.com/
- XigmaNAS: https://www.xigmanas.com/
- pfSense: https://www.pfsense.org/