



LINUXOWYCH

LIFEHACKÓW



Marcin Gąstól

60 LINUXOWYCH LIFEHACKÓW

Spis treści

Powłoka i terminal	9
1. Uruchomienie ostatniego polecenia z uprawnieniami administratora (sudo !!)	9
2. Wykorzystanie historii poleceń (!)	10
3. Szybka zamiana w poprzednim poleceniu (^stare^nowe)	11
4. Rozszerzenie nazw za pomocą klamr (brace expansion)	12
5. Wykorzystanie parametrów powłoki (parameter expansion)	13
6. Podstawienie procesu (process substitution)	14
7. Kontrolowanie zadań w tle (job control)	14
8. Odłączanie procesu od terminala (nohup i disown)	15
9. Personalizowany kolorowy prompt (PS1)	16
10. Użycie terminalowego multipleksera (tmux/screen)	17
System plików i zarządzanie plikami	20
11. Wykonywanie akcji na wynikach wyszukiwania (find -exec)	20
12. Wyszukiwanie największych i najnowszych plików (find -size, -mtime)	21
13. Przyspieszanie operacji na wielu plikach (xargs -P)	22
14. Synchronizacja i kopie zapasowe katalogów (rsync)	23

15. Szybka kompresja i archiwizacja (tar z kompresją)	24
16. Sprawdzenie, który proces używa pliku lub portu (lsof)	25
17. Monitorowanie zmian w systemie plików (inotifywait)	25
18. Tworzenie obrazu dysku za pomocą dd (z podglądem postępu)	26
19. Lokalizowanie największych katalogów (du + sort)	27
20. Montowanie obrazów dysków i ISO (opcja loop)	28
Zarządzanie systemem i procesami	30
21. Zmiana priorytetu procesu (nice i renice)	30
22. Kontrola obciążenia dysku przez proces (ionice)	31
23. Przypisanie procesu do określonego CPU (taskset)	32
24. Wysyłanie sygnałów do procesów (kill, killall)	32
25. Okresowe odświeżanie wyników poleceń (watch)	33
26. Śledzenie wywołań systemowych (strace)	34
27. Sprawdzanie zależności bibliotek (ldd)	35
28. Awaryjne sterowanie systemem (Magic SysRq)	36
29. Analiza czasu startu systemu (systemd-analyze)	37
30. Jednorazowe zaplanowanie zadania (at)	38
Sieć i zdalny dostęp	40
31. Tunelowanie portów przez SSH (ssh -L/-R)	40
32. Dynamiczne proxy SOCKS przez SSH (ssh -D)	41
33. Logowanie bez hasła za pomocą kluczy SSH (ssh-keygen, ssh-agent)	42

34. Montowanie zdalnych katalogów przez SSHFS	43
35. Kopiowanie katalogów przez sieć za pomocą tar + SSH	44
36. Błyskawiczny transfer plików za pomocą netcat	45
37. Skanowanie sieci i portów (nmap)	46
38. Szybkie udostępnienie plików przez HTTP (wbudowany serwer Pythona)	47
39. Udostępnianie połączenia internetowego (iptables NAT)	48
40. Sprawdzanie otwartych portów i połączeń (netstat/ss)	49
Bezpieczeństwo systemu	51
41. Wyszukiwanie plików z ustawionym bitem SUID/SGID	51
42. Rozszerzone listy kontroli dostępu (setfacl)	52
43. Szyfrowanie plików za pomocą GPG	53
44. Sprawdzanie integralności plików (sumy kontrolne)	54
45. Generowanie losowych haseł lub danych (openssl rand)	55
46. Automatyczna ochrona przed atakami brute-force (fail2ban)	56
47. Prosta konfiguracja zapory sieciowej (ufw)	58
48. Kontrolowanie domyślnych uprawnień nowych plików (umask)	59
49. Utwardzenie konfiguracji SSH (wyłączenie haseł i root)	60

50. SELinux / AppArmor – dodatkowa warstwa bezpieczeństwa	61
Automatyzacja i skrypty	64
51. Masowe zamiany tekstu w plikach (sed)	64
52. Przetwarzanie danych tekstowych (awk)	65
53. Pętle shellowe w jednej linii (for)	66
54. Wielolinijkowe wejście w skryptach (here document)	67
55. Cykliczne zadania w tle (cron)	68
56. Obsługa sygnałów w skryptach (trap)	69
57. Rozdzielanie wyjścia do pliku i dalej (tee)	70
58. Śledzenie zmian konfiguracji za pomocą Git	71
59. Wykorzystanie curl do automatyzacji żądań webowych	72
60. Zaawansowane wyszukiwanie tekstu (grep)	73
Podsumowanie	76

Witam serdecznie!



Nazywam się Marcin Gąstół i jestem **ekspertem Linux Magazine** oraz **Inżynierem DevOps**

Na co dzień zajmuję się automatyzacją, optymalizacją pracy w systemie Linux oraz odkrywaniem sprytnych rozwiązań, które pozwalają wycisnąć z terminala maksimum możliwości.

Z tą myślą powstał **ebook „Linux Lifehacks”** – zbiór 60 zaawansowanych technicznych „hacków” dla doświadczonych użytkowników systemu Linux. Porady zostały pogrupowane tematycznie, aby ułatwić nawigację po różnych obszarach zaawansowanego użytkownika systemu.

Każdy hack zawiera tytuł, opis zastosowania, przykładową komendę lub kod, a w razie potrzeby również uwagę o specyfice różnych dystrybucji Linuxa. Dzięki temu dowiesz się, jak efektywniej korzystać z powłoki i terminala, zarządzać plikami i systemem plików, administracją systemu i procesami, siecią oraz bezpieczeństwem, a także automatyzacją i skryptami.

Wszystkie przedstawione hacki zakładają podstawową znajomość Linuxa i kierowane są do użytkowników o zaawansowanym poziomie umiejętności, którzy chcą usprawnić swoją pracę poprzez sprytnie sztuczki i mniej znane funkcje.

Jeśli chcesz być na bieżąco z kolejnymi technicznymi materiałami, wskazówkami i nowinkami ze świata open source — **dołącz do naszej społeczności!**

 Obserwuj nas na Facebooku: facebook.com/linuxmagazinepl

 Odwiedź naszą stronę: linux-magazine.pl

 [Zadaj mi pytanie](#)

Powłoka i terminal

1. Uruchomienie ostatniego polecenia z uprawnieniami administratora (sudo !!)

Często zdarza się, że wydajemy polecenie wymagające uprawnień administratora (root), zapominając poprzedzić je komendą sudo. Zamiast wpisywać ponownie całe polecenie z sudo, oferuje skrót **!!**, który oznacza „ostatnie polecenie”. Po nieudanej próbie z powodu braku uprawnień można szybko powtórzyć ją z prawami root, wpisując **sudo !!**

```
$ apt install apache2
```

```
E: Nie udało się otworzyć pliku /var/lib/dpkg/status – Permission denied
```

```
$ sudo !!
```

```
sudo apt install apache2
```

```
[sudo] hasło użytkownika:
```

```
... (instalacja przebiega) ...
```

Skrót **!!** działa w powłoce oraz wielu innych powłokach zgodnych z em (np. Zsh). W starszych powłokach lub innych shellach może nie być dostępny.