



Konf. i Zabezp. Sys. Op. z Rodz. Ubuntu

2020-2026 Wszelkie Prawa Zastrzeżone przez Jacka Marcina Jaworskiego czyli Energo Kodera Atlanta

autor:	Jacek Marcin Jaworski
pseudonim:	Energo Koder Atlant
pomocnicy autora:	ChatGPT
miejsce:	Pruszcz Gd., Polska
utworzono:	2020-07-12, nie.
wersja: 5718 z dnia:	2026-06-26
program składu:	Libre Office Writer
sys. op.:	Kubuntu, Triskel
źródło:	energokod.gda.pl

Ten dok. w wer. PDF jest podpisany cyfrowo wolnym prog. GNU gpg dostępnym bezpłatnie ze s. www.gnupg.org/download. Instrukcja w j. pol. jak się posługiwać prog. GNU gpg w sys. op. Linuks z rodz. Debian/Ubuntu znajduje się w całkowicie bezpłatnym dok. PDF [Konf. i Zabezp. Sys. Op. z Rodz. Ubuntu](#) w roz. "Podpisywanie Dok. PDF".

Spis treści

Streszczenie.....	4
O Autorze.....	4
Treść Tej Monografii.....	5
Cele Tej Monografii.....	5
Założenia Wstępne.....	6
Grupa Docelowa.....	6
Czego Nie Opisałem w Tej Monografii.....	6
Brak Gwarancji 100% Bezpieczeństwa Sys. Op.....	6
Forma Tej Monografii.....	6
Skróty.....	6
Konwencje w Tekście.....	7
Podstawowe Skróty Edytora Tekstu Nano.....	8
1 Mechanizmy Bezpieczeństwa w Sys. Op. Linuks.....	8
1.1 Logiczny Podział Dysku Twardego: Partycje i Plik /etc/fstab.....	8
1.2 Użytkownicy w Sys. Op. Linuks.....	9
1.3 Sys. Uprawnień w sys. op. Linuks.....	10
1.4 Piaskownice.....	11
1.4.1 AppArmor - To Nie Piaskownica, Ale.....	11
1.4.2 Piaskownice w Paczkach Snap i Flatpack.....	11

1.4.2.1 Snap.....	11
1.4.2.2 Flatpack.....	12
1.4.3 AppImage.....	12
1.4.4 Piaskownica Firejail.....	12
1.4.5 Porównanie Piaskownic.....	13
1.5 Zapory Sieciowe.....	13
1.6 Co Jest Nie Tak z VPN?.....	13
1.7 Co Jest Nie Tak z Siecią Tor?.....	14
2 Budowa Sieci Internet.....	14
2.1 Struktura Sieci Internet.....	14
2.2 Protokoły w Sieci Internet.....	14
2.2.1 Protokół IP.....	14
2.2.2 Protokół UDP.....	14
2.2.3 Protokół TCP.....	14
2.2.4 Porty w UDP i w TCP.....	15
2.3 Sieć Lokalna.....	15
2.4 NAT Czyli Lokalna Brama Do Globalnej Sieci Internet.....	15
2.5 Sieć Globalna, Czyli Internet.....	16
2.6 Nazwy Domen a IP.....	16
3 Wybór Modelu Bezpieczeństwa w Pracy z Sys. Op. Linuks.....	16
3.1 Domowa Stacja Robocza - Sys. Online.....	16
3.2 Firmowa Stacja Robocza - Sys. Offline z Lustrzanym Repo w Sieci Lokalnej.....	17
4 Przygotowanie Do Instalacji Sys. Op. Linuks.....	18
4.1 Jaką Dystrybucję Wybrać?.....	18
4.1.1 Smaki Ubuntu.....	18
4.1.1.1 Oficjalne smaki Ubuntu.....	18
4.1.1.2 Popularne nieoficjalne smaki (remiksy).....	19
4.1.1.3 Popularne nieoficjalne pochodne Ubuntu.....	19
4.1.2 Który [Smak Ubuntu - przyp. JMJ] wybrać?..	19
4.1.3 Oficjalne odmiany Ubuntu Server.....	19
4.1.3.1 Popularne nieoficjalne odmiany i pochodne.....	20
4.1.3.2 Projekty oparte bezpośrednio na Ubuntu Server.....	20
4.1.3.3 Dla jakich zastosowań?.....	20
4.1.4 Wybierz Dystrybucję Typu LTS.....	20
4.1.5 Są Dystrybucje Bez Zamkniętych Pakietów - Ale Czy Warto Je Instalować?.....	21
4.2 Jak Prawidłowo Zainstalować Sys. Op. Linuks Mając Tylko Skompromitowany Sys. Komp.....	21
4.3 Pobieranie Obrazu instalki Sys. Op. Linuks.....	21
4.3.1 Pobranie Sum Kontrolnych.....	21
4.3.2 Odłącz Komp. Od Sieci.....	21
4.3.3 Spr. Pobranego Obrazu.....	21
4.3.4 Nagrywanie Obrazu.....	22
4.3.4.1 Rozpoznawanie Napędów w Sys. Op. Linuks.....	22
4.3.4.2 Zapis Obrazu Na Patyk USB.....	22
4.4 Uruchomienie Instalki.....	22
4.5 Partycjonowanie Dysku.....	22
4.6 Pamięć Wymiany.....	24
4.7 Generowanie Silnego Hasła.....	25
4.7.1 cracklib-check.....	25
4.7.2 John The Ripper.....	25
4.7.3 Zmiana Hasła.....	26
5 Instalacja Sys. Op. Linuks.....	26

5.1 W Czasie Instalacji Sys. Op. Nie Łącz Się z Siecią Lokalną Ani z Siecią Internet.....	26
5.2 Wybierz Punkty Montowania Przygotowanych Partycji.....	26
5.3 Wprowadź Hasło Jakie Wygenerowałeś.....	26
6 Konf. Stacji Roboczej Linuks Po Instalacji.....	26
6.1 Skonfiguruj sudo.....	26
6.1.1 Dodaj Siebie Do Grupy sudo.....	26
6.1.2 Ustaw sudo Tylko Dla Siebie.....	27
6.1.3 Włącz Sobie Użycie sudo Bez Hasła.....	27
6.2 Skonfiguruj Zaporę Sieciową UFW.....	27
6.2.1 Domyślne Blokowanie Ruchu Sieciowego Przychodzącego.....	27
6.3 Konfiguracja Prog. Gł. Sys. Op. Linuks.....	27
6.4 Skonfiguruj Partycje.....	28
6.5 Wyłącz Plik Wymiany.....	28
6.6 Włącz Automatyczne Ubijanie Zbyt Żarłocznego Procesu.....	28
6.7 Zaostrz Prawa Dostępu Do Katalogów Użytkowników.....	29
6.7.1 Katalogi Domowe.....	29
6.7.2 UMASK.....	30
6.7.2.1 UMASK Globalny.....	30
6.7.2.2 Problemy z Globalnym UMASK.....	30
6.7.2.3 UMASK Lokalny.....	30
6.7.3 DIR_MODE.....	30
6.8 Wyłącz Konsolę Dla Nowych Użytkowników.....	31
6.9 firejail.....	31
6.9.1 Instalacja firejail.....	31
6.9.2 Włączenie firejail.....	31
6.9.3 Uruchamianie Prog. w Piaskownicy firejail i Bez Niej.....	31
6.9.4 Spr. Czy Prog. Jest Uruchomiony w Piaskownicy firejail.....	32
6.9.5 Strojenie firejail.....	32
6.9.6 Dodawanie Brakujących Profili firejail.....	34
6.9.6.1 Aut. Tworzenie Nowego Profilu firejail	34
6.9.6.2 Ręczne Tworzenie Nowego Profilu firejail.....	34
6.9.7 Paczki AppImage.....	35
6.9.8 Globalne Wyłączenie firejail.....	35
6.10 Skonfiguruj Sieć.....	35
6.11 Awaryjne Połączenie z Siecią Internet.....	36
6.12 Instalacja i Konf. Demona CUPS.....	37
6.13 SSH.....	38
6.13.1 Instalacja ssh.....	38
6.13.2 Wygeneruj Parę Kluczy.....	38
6.13.3 Załaduj Publiczne Klucze SSH Na Serwer	38
6.14 Postarzenie Prog. Gł. Sys. Op. Linuks.....	38
6.14.1 Blokada Aktualizacji Prog. Gł. Sys. Op. Linuks.....	38
6.14.2 Instalacja Najstarszego Prog. Gł. Sys. Op. Linuks w Repo.....	39
6.14.3 Uruchom Ponownie Sys. Komp. Wybierając w boot menu Starą Wer. Prog. Gł. Sys. Op. Linuks.....	39
6.14.4 Usuwanie Zbędnych Prog. Gł.....	39
6.15 Konfiguracja Stacji Roboczej Linuks Dla Programisty.....	39
6.15.1 Włącz Zrzuty Obrazów Pam. Prog.....	39
6.16 Konfiguracja Komp. z sys. op. Linuks Dla Nie Programisty.....	40
6.16.1 Wyłącz zrzuty prog. gł. i pozostałych prog.	40
6.17 Ważne Pliki Sys. Op. Linuks.....	40
6.18 Zbędni Użytkownicy.....	40
6.19 Zbędne Grupy Użytkowników.....	40
6.20 Pliki Bez Właściciela.....	40
6.21 Uszkodzone Linki Symboliczne.....	41
7 Konf. Serwera Linuks Po Instalacji.....	41
7.1 Skonfiguruj sudo Tak Jak w Roz. 6.1.....	41
7.2 Skonfiguruj Zaporę Sieciową Tak Jak w Roz. 6.2	41
7.3 Instalacja i Konf. Demona sshd.....	41
7.3.1 Konf. demona sshd.....	41
7.3.2 Dla chętnych: ssh-audit.....	42
7.4 Instalacja i Konf. Sys. Wersjonowania Git.....	42
7.4.1 Założenia Serwera Git.....	42
7.4.2 Instalacja git.....	42
7.4.3 Tworzenie Kont Programistów Na Serwerze	42
7.4.4 Tworzenie Kat. z Repo Na Serwerze.....	42
7.4.5 Schemat Pracy z Serwerem Git.....	43
7.4.5.1 Tworzenie Nwego Repo Produkcyjnego Na Kompie Lidera.....	43
7.4.5.2 Tworzenie Nowego Lokalnego Repo Git Na Kompie Lidera.....	43
7.4.5.3 Pobieranie Repo Na Kompa "Zwykłego" Programisty John.....	43
7.4.5.4 Praca Na Kompie "Zwykłego" Programisty John.....	43
7.4.5.5 Lider Dociąga <i>john/master</i>	44
7.5 Instalacja i Konf. Lustrzanego Repo.....	44
7.5.1 Instalacja Potrzebnych Pakietów.....	44
7.5.2 Przygotowanie Kat. z Lustrzanym Repo..	44
7.5.3 Konf. apt-mirror.....	44
7.5.4 Pobieranie Zdalnego Repo (Tworzenie Lustrzanego Repo).....	45
7.5.5 Przetaw Stacje Robocze Na Pracę z Lustrzanym Repo.....	45
7.6 Instalacja i Konf. Demona CUPS z Drukarką USB	45
7.6.1 Instalacja CUPS na serwerze.....	45
7.6.2 Konf. CUPS na serwerze.....	45
7.6.3 Instalacja Sterownika USB Dla Brother MFC-L2752DW Na Serwerze.....	46
7.6.4 Włączenie Współdzielenia w CUPS Na Swerwerze.....	46
7.6.5 Sprawdzanie Drukarki z Serwera.....	46
7.6.6 Sprawdzenie Drukarki z Kompa Klienta..	46

7.6.7 Konf. Dostępu Klienta Do "Usieciowionej" Drukarki USB.....	46	9.4 Skaner Debsecan (Poszukuje exploit-ów).....	55
7.7 Instalacja i Konf. Demona Samba.....	47	9.4.1 Instalacja.....	55
7.7.1 Instalacja.....	47	9.4.2 Skanowanie i Interpretacja Wyników.....	55
7.7.2 Konf. smb.....	47	9.5 Skaner Fail2ban (Pokazuje Nieudane Próby Logowania).....	56
7.7.3 Testy smb.....	47	10 Automatyzacja Monitorowania Bezpieczeństwa.....	56
7.7.4 Montowanie Dysków Samby:.....	47	10.1 Monitorowanie II. Wywołań Prog. i Skryptów.....	56
7.8 Demon NFS.....	48	11 Skryte Korzystanie z Sys. Op. Linuks.....	56
8 Diagnostyka Sys. Op. Linuks.....	48	11.1 Skrypt Czyszczący.....	56
8.1 memtest86+.....	48	12 Skryte Korzystanie z Sieci Internet.....	57
8.2 uname.....	48	12.1 Przeszkody w Skrytym Korzystaniu z Internetu	57
8.3 dmesg.....	48	12.1.1 Przeglądarki Mają Pełen Dostęp Do Kat. Domowych Wszystkich Użytkowników w sys. op. Linuks.....	57
8.4 etckeeper.....	48	12.1.2 Wysyłanie ID Sys. Op. i ID Przeglądarki.....	57
8.5 debsums.....	48	12.1.3 Serwery WWW Blokują Klientów Wychodzących z Sieci Tor.....	58
8.6 systemctl.....	49	12.1.4 Dostawcy ISP Publikują Zakresy Swoich Adresów IP.....	58
8.7 journalctl.....	49	12.1.5 Dostawcy Internetu Handlują Historią Odwiedzanych s. WWW.....	58
8.8 Diagnostyka Dysków w Sys. Op. Linuks.....	49	12.1.6 Brak Manifestów Do s. HTML.....	58
8.8.1 efibootmgr.....	49	12.2 Serwery DNS.....	59
8.8.2 smartctl.....	49	12.3 Tor Browser.....	59
8.8.3 df.....	49	12.4 Poprawa Prywatności w Tor Browser, i w Firefox.....	59
8.8.4 lsblk.....	49	12.4.1 Włącz Kasowanie Całej Historii Przy Zamykaniu.....	60
8.9 Naprawa Dysków w Sys. Op Linux.....	49	12.4.2 Zainstaluj Dodatek HTTPS Everywhere...60	
8.9.1 Ważne [Naprawiamy Wył. Dyski Niezamontowane - przyp. JM].....	50	12.4.3 Zainstaluj Dodatek Privacy Badger.....60	
8.9.2 Sprawdzenie Systemu Plików Niezamontowanej Partycji.....	50	12.5 Przeglądarka Chromium.....	60
8.9.3 Automatyczna Naprawa Znalezionych Błędów.....	50	12.6 Poprawa Prywatności w Chromium i Chrome	60
8.9.4 Wymuszenie Pełnego Sprawdzenia.....	50	12.6.1 Włącz Kasowanie Całej Historii Przy Zamykaniu.....	60
8.9.5 Typowy Sposób [Postępowania - przyp. JM] Podczas Problemów z Systemem.....	50	12.6.2 Zainstaluj Dodatek HTTPS Everywhere...60	
8.9.6 Sprawdzenie Wszystkich Systemów Plików z /etc/fstab.....	50	12.6.3 Zainstaluj Dodatek Privacy Badger.....60	
8.10 Diagnostyka Sieci w Sys. Op. Linuks.....	51	12.6.4 Autouzupełniaj Wyszukiwania i Adresy URL.....	60
8.10.1 ip.....	51	12.6.5 Ulepsz Wyszukiwanie i Przeglądanie.....61	
8.10.2 whois.....	51	12.6.6 Wysyłaj Żądanie „Bez Śledzenia” Podczas Przeglądania.....	61
8.10.3 dig.....	51	12.6.7 Kontynuuj Działanie Aplikacji w Tle Po Zamknięciu Chromium.....	61
8.10.4 resolvelctl.....	51	12.7 Inne Przydatne Dodatki.....	61
8.10.5 ss.....	51	12.7.1 I don't care about cookies.....	61
8.10.6 tcpdump.....	52	12.7.1.1 Tor Browser i Firefox.....	61
8.10.7 arp-scan.....	52	12.7.1.2 Chromium i Chrome.....	61
8.10.8 nmap.....	52	12.7.2 Otwieranie Linku i Przejście Do Nowej Karty Jednym Młaskiem Środkowego Przycisku Pyszy.....	61
8.10.9 Tab.: Skanery Sieciowe.....	52	12.7.2.1 Tor Browser i Firefox.....	61
9 Ręczna Diagnostyka Bezpieczeństwa.....	53	12.7.2.2 Chromium i Chrome.....	61
9.1 Testy Zapory Sieciowej.....	53	12.8 Wyszukiwarki.....	61
9.1.1 Test Skanowania Portów.....	53	12.8.1 Brave Sarch.....	61
9.1.2 Test Dostępu Do Otwartego Portu Zablokowanego Przez UFW.....	54	12.8.2 Google.com.....	61
9.2 Skaner Lynis (Skaner Bezpieczeństwa).....	54		
9.2.1 Instalacja.....	54		
9.2.2 Skanowanie.....	54		
9.2.3 Interpretacja Wyników.....	54		
9.3 Skaner Rkhunter (Poszukuje Rotkitów).....	55		
9.3.1 Instalacja.....	55		
9.3.2 Aktualizacja.....	55		
9.3.3 Skanowanie.....	55		
9.3.4 Interpretacja wyników.....	55		

12.8.3 Tab.: Porównanie Brave Search i Google.com.....	62
12.8.4 Tab.: Inne Wyszukiwarki z Własnym Indekssem.....	62
13 Poczta el.....	62
13.1 Podpisywanie i Szyfrowanie Poczty El.....	62
13.2 Niezbędna Konf. Klienta Poczтового Thunderbird (w j. ang. Thunderbird).....	62
13.2.1 Triki Pozwalające Częściowo Uzdrożyć Thunerbird.....	62
14 Podpisywanie Dok. PDF.....	63
15 Komunikacja z Androidem Przez adb.....	64
15.1 Instalacja adb w Linuksie.....	64
15.2 Przygotowanie Telefonu.....	64
15.3 Sprawdzenie Połączenia.....	64
15.4 Podstawowe Czynności.....	65
15.5 <i>Najczęściej Używane Polecenia [adb - przyp. JM]</i>	65
15.6 Wykonywanie Pojedynczych Poleceń.....	65
15.7 <i>Powłoka Linuksa w Telefonie</i>	65
15.8 Kopiowanie Plików.....	65
15.8.1 Z Telefonu Do Komputera.....	65
15.8.2 Z Komputera Do Telefonu.....	65
15.9 Lista Aplikacji.....	65
15.10 Instalowanie Aplikacji APK.....	65
15.11 Zrzut Ekranu.....	66
15.12 Nagranie Ekranu.....	66
15.13 <i>Sprawdzanie Stanu Baterii</i>	66
15.14 Rejestrowanie Logów Systemowych.....	66
15.15 Restart Urządzenia.....	66
15.16 Połączenie Przez Wi-Fi.....	67
15.17 Przekierowanie portów.....	67
15.18 Dostęp Root.....	67
15.19 Czego nie można zrobić bez roota?.....	67
16 Lektura Uzupełniająca i Bibliografia.....	67
17 Podziękowania.....	68
18 Licencja.....	68

Streszczenie

Niniejsza monografia opisuje następujące zagadnienia dotyczące konf. i zabezpieczenia stacji roboczej z sys. op. Linuks (Ubuntu i pochodne), oraz serwerów Linuks (Ubuntu Serwer i pochodne):

- Budowa sieci Internet;
- Niebezpieczeństwa związane z korzystaniem z sieci Internet;
- Bezpieczeństwo w sieci lokalnej;
- Mechanizmy bezpieczeństwa w sys. op. Linuks;
- Koncepcja użycia komputera z sys. op. Linuks działającego w sieci Internet;

- Przygotowania do instalacji sys. op. Linuks;
- Instalacja sys. op. Linuks;
- Konf. Stacji Roboczej z sys. op. Linuks;
- Konf. Serwera z sys. op. Linuks;
- Diagnostyka sys. op. Linuks;
- Diagnostyka i naprawa dysków w sys. op. Linuks;
- Diagnostyka sieci w sys. op. Linuks;
- Ręczna diagnostyka bezpieczeństwa sys. op. Linuks;
- Automatyzacja monitorowania bezpieczeństwa w sys. op. Linuks;
- Skryte korzystanie z sys. op. Linuks;
- Skryte korzystanie z sieci Internet;
- Podpisy cyfrowe dok. PDF;
- Komunikacja z Androidem przez USB i adb.

Miejmy świadomość, że ta monografia powstała tylko z dwóch powodów:

- 1. Tysiącom polskich adminów jest wszystko jedno co się dzieje z waszymi kompami;**
- 2. Mi nie jest wszystko jedno!**

O Autorze

Od ur. w 1978 r. w Gd. żyję w Pruszczu Gd. na ul. Spacerowej. Od 2020-06-20 do 2021-06-19 mieszkałem w Gdyni na ul. Komandorskiej (po roku wróciłem do Pruszcza Gd.).

Programuję komputery od lut. 1997 r. od 1999 r. mam tytuł Technika Elektronika spec. Systemy Komputerowe. Zaliczyłem 3 lata studiów informy na PG (jednak dyplomu inż. nie zrobiłem). Legalną maturę zdałem w 2016 r. Jednak po 2005 r. wprowadzono w całej Polsce zmiany w prog. studiów zaocznych (wymuszono na wszystkich kier. 7 sem. z j. ang.) powoduje to, że nie jestem w stanie ich zaliczyć.

W latach 1999-2007 (jednak bez ciągłości zatrudnienia) byłem programistą aplikacji w C++ dla sys. Windows.

W latach 2017-2022 (jednak bez ciągłości zatrudnienia) byłem programistą aplikacji w C++ na sys. Linuks i Android.

Jeśli chodzi o mój kierunek rozwoju, to chcę być jak najlepszym inżynierem i architektem sys. i to nie tylko komputerowych.

Moje zainteresowania zawodowe to przede wszystkim:

*Studia nad architekturą wzorcowych sys. komp.*Studia nad nowymi algorytmami (jednak nie SI)*Studia nad bezpieczeństwem współczesnych sys. komp.*Studia nad prywatnością użytkowników współczesnych sys. komp.*Podnoszenie jakości, efektywności i bezpieczeństwa w pracy przez realizację racjonalizatorskich projektów *

*Programowanie w językach: Asembler, C, C++ i D.

Wystrzegam się jak mogę „produktów” wielkich korporacji z niejawnych (zło jest niejawne) powodów zwykle wynajdują patologiczne wynalazki¹.

Jestem poszukiwaczem i kolekcjonerem "dobrych zasad życiowych" i "dobrych zasad inżynierskich". Dzięki tym związyłem, hasłowym zasadom często widzę sens podejmowania większego wysiłku by uzyskać obiektywnie dobry efekt zamiast stosowania półśrodków.

Zdrowe zasady pozwalają zostawiać za sobą działające rozwiązania zamiast partactw.

Jestem praktykującym zwolennikiem filozofii dobra i moralności, czyli Totalizmu. Z filozofią Totalizmu, w wyd. prof. Jana Pająka z NZ, po raz pierwszy zetknąłem się w Sieci Internet 2002r. (od końca 2001r. mam stały dostęp do Internetu) i od razu b. się nią zafascynowałem i tak jest do d. dzisiejszego. Od 2020r. rozwijam jej popr. wer. w postaci [Ideologii Geniuszy-Mocarzy](#). Mój Totalizm różni się od Totalizmu prof. Jana Pająka z NZ tym, że ja uważam że Totalizm składa się z dobra i z moralności, a nie z samej moralności. Wynika to z fak-

¹ Jak wiecie język C i sys. **Uniks** stworzyło 2 ludzi: **Dennis Ritchie** i **Ken Thompson**. Dlatego jestem na 100% pewien, że gdyby ich projekt był prowadzony z rozmachem w stylu wielkich korporacji, to: a) Język C nigdy by nie powstał, b) **Uniks** nigdy by nie powstał, c) powstały by potwory podobne do **Ada**, **Jawa**, **C#**, **Windows** i **Android**.

Jak zauważył prof. Jan Pajak z NZ: W organizacjach pasożytniczych wszystkie złe pomysły pojawiają się od górnicy, a wszystkie postępowe koncepcje powstają oddolnie.

tu, że sama moralność bez dobra prowadzi do filozofii moralności i zła czyli w istocie do filozofii nazistowskiej.

W latach 2004-2013 5x siedziałem w psychiatryku. Sądy i lekarze byli i są jednomyślni że jestem b. chory psychicznie, na przekór braku jakichkolwiek dowodów mojego rzekomego szaleństwa. Za "dowody" mojego szaleństwa lekarze uznają to, że otaczających mnie ludzi mam za "wrogich szatańskich pasożytów" i że po wzmocnionych dawkach leków psychotropowych (bo w szpitalach mogą dawać mocniejsze dawki) spałem całymi dniami - nazwali to "zespołem katatonicznym - paranoidalnym w przebiegu schizofrenii".

W d. 2025-06-17, wto. sąd rej. w Gd. skazał mnie na 6. odsiadkę w psychiatryku bez udowodnienia mi żadnych win oraz wcale nie odnosząc się do mojej obronnej argumentacji jasno wykazującej że to oskarżenie (personel domowy i medyczny) "ma coś z dekletem" a nie ja. Sąd okręgowy w Gd., na posiedzeniu niejawnym, w d. 2025-10-27, pon. odrzucił moją apelację bez jej rozpatrzenia i podtrzymał wyrok sądu rej. Co dziwne tego wyroku na razie nikt nie wyegzekwował (piszę to w d. 2026-06-26, pią.). Przejawy mojej dyskryminacji oraz odrzuconą apelację do sądu okręgowego przytaczam w: [2025-10-06 Do Amnesty International Polska - Prośba o Pomoc Dla Prześladowanego Jacka Marcina Jaworskiego.pdf](#).

Od 2024-12-20, pią. prowadzę moją domową s. WWW: [energokod.pl](#). Od jesieni 2025 r. jest ona dostępna pod nowym adresem [energokod.gda.pl](#). Na tej s. WWW pub. kilkadziesiąt dok. PDF o tematyce totaliztycznej, Mini Netykietę i moje dane kontaktowe.

Treść Tej Monografii

Cele Tej Monografii

1. Stworzenie dobrego, sprawdzonego i szybkiego do wdrożenia przepisu na prawidłową konfigurację stacji roboczej i serwera z sys. op. Linuks w domu i w pracy;
2. Stworzenie dobrego, sprawdzonego i szybkiego do wdrożenia przepisu na prawidłową konfigurację sieci domowej;

3. Propagowanie wiedzy o sys. op. Linuks i o sieci Internet.

Założenia Wstępne

Aby osiągnąć wyżej postawione cele muszę przyjąć pewne założenia:

1. Komputer działa normalnie i fizycznie jest bezpieczny², czyli jest godny zaufania;
2. Instalowana jest dystrybucja sys. op. Linuks to Ubuntu lub ich pochodne;
3. Prog. gł. sys. op. Linuks działa normalnie i nie zawiera tylnych furtek³, czyli jest godny zaufania;
4. Programy narzędziowe: sha256, dig, whois, ufw i firejail działają normalnie i nie zawierają tylnych furtek, czyli są godne zaufania;
5. Aplikacje działające w przestrzeni użytkownika mogą mieć tylne furtki, czyli nie są godne zaufania.

Grupa Docelowa

Grupa docelowa to użytkownicy sys. op. Linuks którzy chcą zmaksymalizować swoje bezpieczeństwo, prywatność i wydajność podczas korzystania ze swoich stacji roboczych wpiętych do sieci Internet.

W szczególności obejmuje to osoby:

- Entuzjaści sys. op. Linuks - głównie użytkownicy domowi;
- Programiści pracujący na co dzień z sys. op. Linuks;
- Pozostali zawodowi użytkownicy sys. op. Linuks nie będący administratorami ani programistami.

Czego Nie Opisałem w Tej Monografii

Nie udaję, że znam się na wszystkich odmianach sys. op. Linuks, dlatego piszę tylko o dystrybucji Ubuntu i pochodnych, bo ich na co dzień używam.

Nie poruszam kwestii usług VPN, bo uważam że tylko spawalniają dostęp do sieci. Bo nie ma co wierzyć, że dostawca VPN „jest niezależny” i wolny od układów z ze "służbami" lub z "tajną policją".

Nie poruszam kwestii skanerów w czasie rzeczywistym takich jak Snort, bo po prostu wiara, że włamywacz będzie tak miły, że pozwoli wysłać wiad. el. że coś się złego dzieje, to jakaś kompletna głupota. A tak działają te sys.

Brak Gwarancji 100% Bezpieczeństwa Sys. Op.

Starłem się opracować jak najlepszą instrukcję zasad pracy z sys. op. Linuks głównie po to by samemu z niej korzystać w domu i w pracy. Jednak nie będę ukrywał, że zagadnieniami bezpieczeństwa informatycznego zajmuję się głównie po godzinach. Dlatego:

AUTOR NIE BIERZE ODPOWIEDZIALNOŚCI ZA WYKONYWANIE PONIŻSZYCH CZYNNOŚCI NA KOMPUTERZE CZYTELNIKA.

AUTOR NIE GWARANTUJE 100% BEZPIECZEŃSTWA sys. op. Linuks PO ZASTOSOWANIU PONIŻSZYCH INSTRUKCJI.

AUTOR NIE GWARANTUJE 100% PRYWATNOŚCI W INTERNECIE PO ZASTOSOWANIU PONIŻSZYCH INSTRUKCJI.

Forma Tej Monografii

Skróty

Na potrzeby tej monografii wprowadzam wygodne skróty myślowe:

2 Czyli nie ma konieczności szyfrowania partycji.

3 W j. ang.: back doors

intruz	włamywacz komputerowy lub inaczej kraker lub inaczej "etyczny haker" czyli kanalia na etacie rządowym. Osoba ta włamuje się zarówno przez sieć, i gdy ma fizyczny dostęp do komputera
prog. gł.	program główny = jądro = w j. ang. kernel
Linuks	Ubuntu
sys. komp.	system komputerowy, komputer lub sterownik mikroprocesorowy
konsola	emulator terminala Konsole lub Terminal lub XTerm
\$USER	twój login w sys. op. Linuks
\$HOME	twój katalog domowy w sys. op. Linuks. Czyli /home/\$USER;
\$TWOJE_IP	twoje IP: takie jakie sobie wymyślisz i takie jakie zwraca polecenie ip a po poprawnej konfiguracji sieci
edytor	edytor tekstu Nano
art.	artykuł
aut.	autor
d.	dzień
dok.	dokument
el.	element
ew.	ewentualnie
f.	funkcja
GB	akronim z j. ang. Great Britain
gł.	główny
il.	ilość
inż.	inżynier
IP	akronim z j. ang.: Internet Protocol
j.	język
j. ang.	język angielski
j. pol.	język polski
jw.	jak wyżej
kat.	katalog
kol.	kolejność
ks.	książka
m. in.	między innymi
np.	na przykład
o.	obiekt
odp.	odpowiedź
org.	oryginalny

ost.	ostatni
p.	punkt
pam.	pamięć
PDF	akronim z j. ang.: Portable Document Format
pow.	powyżej
pub.	publikacja, publikować
pyt.	pytanie
r.	rok
roz.	rozdział
s.	strona
spr.	sprawdzenie
sys. op.	system operacyjny
tel.	telefon
tł.	tłumacz, tłumaczenie
twz.	tak zwany
ul.	ulica
uż.	użytkownik
wer.	wersja
wew.	wewnętrzny
wg.	według
wł.	włączyć
wyd.	wydanie
wył.	wyłączyć
zaw.	zawartość

UWAGA: Skróty 4 literowe i dłuższe uważam za oczywiste.

Konwencje w Tekście

- Myślę po polsku, mówię po polsku, od urodzenia mieszkam w Polsce, więc piszę i programuję po polsku.

Piszę Linuks, bo w szkole podstawowej uczono mnie, że w polskim alfabecie nie ma x – jego rolę pełni ks. Więc logiczne jest, że pisząc po polsku używam wyłącznie polskiego alfabetu;

Obcych nazw takich jak Linuks, Ubuntu, Internet nie odmieniam przez przypadki, bo logiczne jest, że obce słowa nie podlegają polskim zasadom odmiany przez przypadki;

Wszędzie gdzie to możliwe stosuję polskie terminy techniczne i dla jasności podaję jak się je pisze w j. ang.

- Nie używam upiększających znaków dolara przed poleceniami, by zwiększyć szybkość kopiowania tych poleceń (wystarczy dwumlask⁴);
- Polecenia wymienione w tekście wykonuje się w konsoli/terminalu;
- Objętości plików będę podawał w starym dobrym stylu gdzie 1KB = 1024 bajtów, 1MB = 1KB * 1024, 1GB = 1MB * 1024, 1TB = 1GB * 1024;
- Szybkości transferu danych będę podawał w jednostkach wielkości plików na sekundę. Czyli np. 1MB/s (czyli 1024*1024 bajtów/s), a nie jak podają oszuści 1Mbit/s (czyli 1000 000 / 8 = 125 000 bajtów/s).
- Uwagi krytyczne są w kolorze czerwonym, pogrubione i wyśrodkowane.

Podstawowe Skróty Edytora Tekstu Nano

- Do wprowadzania zmian w sys. będzie nam potrzebny jedynie edytor tekstu. Nano jest chyba dostępny we wszystkich dystrybucjach. A na pewno jest dostępny w Ubuntu.
- Nie zakładam, że znasz j. ang.: więc podam niezbędne skróty klawiszowe edytora Nano:

Zaznacz tekst	Prawy Alt + a
Kopiuj zaznaczony tekst	Prawy Alt + 6
Wklej tekst ze schowka Nano	Ctrl + u
Wklejanie tekstu ze schowka XWindows	Ctrl + Shift + v
Wytnij	Ctrl + k
Zapis pliku	Ctrl + s
Wyjście z edytora Nano	Ctrl + x

Więcej szczegółów można znaleźć w oficjalnym podręczniku [\[nano-podr-pdf\]](#) (w j. ang.).

4 W j. ang.: double click

1 Mechanizmy Bezpieczeństwa w Sys. Op. Linuks

W sys. op. Linuks można wyróżnić hierarchię ograniczeń jakie można nakładać na użytkowników i na uruchamiane prog.:

1. Partycje, plik /etc/fstab: umożliwia zezwolenie użytkownikom na montowanie partycji w sys. plików, umożliwia blokowanie uruchamiania prog. i skryptów, umożliwia blokowanie tworzenia urządzeń blokowych, wyłączenie aktualizacji czasu dostępu do kat. i plików;
 2. Sys. plików atrybuty drwxrwxrwx: umożliwiają nadawanie praw odczytu, zapisu i wykonania na plikach i katalogach. Podział uprawnień jest trójstopniowy: właściciel, grupa i pozostali.
 3. Piaskownica Firejail: Umożliwia ograniczenie dostępu do kat. i plików dla danego prog. uruchamianego przez użytkownika. Działa to w oparciu o mechanizm chroot (prog. widzi spreparowany kat. jako kat. główny czyli "/" (bez cudzysłowu)).
- DLA KAŻDEGO PROG. firejail pozwala na pełne predefiniowanie konf. sieci (łącznie z adresami IP i MAC).**
- Jednak firejail nie pozwala na kontrolę z jakimi adresami IP można się łączyć (to można kontrolować jedynie globalnie w UFW).**
4. Zapora sieciowa UFW: Umożliwia globalną kontrolę w sys. op. gdzie się można łączyć i skąd się można łączyć.

1.1 Logiczny Podział Dysku Twardego: Partycje i Plik /etc/fstab

Dysk komputerowy, HDD, SSD lub NVM, wygodnie jest podzielić na mniejsze, logiczne części i wykorzystywać je do różnych celów.

Wydzieloną, logiczną część dysku nazywamy partycją.

Dzięki temu można zainstalować wiele sys. op. na jednym sys. komp.

Okazuje się, że z punktu widzenia bezpieczeństwa warto mieć specjalne partycje. Umożliwia to kontrolę ważnych katalogów w sys. op.: /boot (prog. gł. sys. op. Linuks), /tmp (pliki tymczasowe) , /var (dane sys. op.), /opt (prog. od zewnętrznych dostawców), /usr/local (prog. i bibl. instalowane w sys. op. przez użytkownika) . Kontrola ta dotyczy przede wszystkim:

1. Kontroli maks. wielkości tych katalogów;
2. Kontroli z jakich partycji można uruchamiać prog.

Plik /etc/fstab definiuje punkty montowania napędów w sys. op. Linuks.

Napędy pojawiają się w sys. jako pliki w kat. /dev natomiast dostęp do ich zawartości uzyskują dopiero gdy je zamontują je do jakiegoś katalogu w sys. plików.

Ten katalog wcześniej nawet nie musi być pusty. Montowanie napędów omówimy na poniższym przykładzie. Wybrałem go bo do montowania tej partycji używałem kilka niestandardowych opcji.

```
UUID=XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX /var          ext2
defaults,noexec,nosuid,nodev          0
2
```

1. Pierwsze pole to nazwa urządzenia lub adres sieciowy dysku. Dawniej w tym miejscu pojawiało się urządzenie z kat. /dev (np.: /dev/hda1). Problem jaki kogoś zabolął, to brak różnicowania napędów w sys. op. Dlatego teraz stosuje się identyfikatory UUID lub LABEL . LABEL to znana z DOS etykieta partycji. Natomiast UUID to wynalazek w sys. op. Linuks który jest rodzajem sumy kontrolnej identyfikującej jednoznacznie daną partycję (nie ma takiej drugiej na Ziemi ani w Kosmosie). Stosowanie LABEL lub UUID daje nam możliwość stosowania dokładnie określonych opcji montowania dla określonych partycji na urządzeniach podłączanych do komp. z sys. op. Linuks.
2. Druga opcja to kat. montowania w sys. plików. Tutaj jest to /var .

3. Trzecia opcja to sys. plików. Tutaj jest to ext2. ext2 nie ma dziennika zmian na dysku, co oznacza, że powinien działać szybciej niż nowsze sys. plików. Ja go stosuję wszędzie tam, gdzie dane się nie zmieniają lub ich utrata nie ma znaczenia.
4. Czwarta opcja to zbiór flag montowania. Tu są to flagi: domyślna, zakaz uruchamiania prog. z tej partycji, brak możliwości tworzenia plików z atrybutem suid (uruchamiania prog. jako właściciel pliku) ani sgid (uruchamiania prog. jako członek grupy właściciela pliku), i brak możliwości tworzenia urządzeń (blokowych ani znakowych) na tej partycji.
5. Piąta opcja jest przeznaczona dla prog. kopii zapasowej i określa czy ma być robiona kopia tej partycji (1) czy nie (0). Tu zaznaczono, że nie ma podlegać archiwizacji.
6. Szósta opcja określa czy sys. plików tej partycji ma być spr. w trakcie uruchamiania sys. operacyjnego. Dla partycji montowanej w korzeniu, czyli w katalogu / powinna to być wartość 1. Natomiast dla pozostałych partycji 2. W dokumentacji nie podano uzasadnienia tej numerologii liczb magicznych.

1.2 Użytkownicy w Sys. Op. Linuks

Główny podział użytkowników w sys. op. Linuks to: root (czyli super użytkownik) i użytkownicy.

Zasada jest taka: root (teoretycznie) może wszystko, użytkownicy mogą tylko tyle by móc normalnie pracować.

Użytkownicy w sys. op. Linuks należą do grup użytkowników. Daje to im różne przywileje. Np. dostęp do stacji dyskietek, napędu CD-ROM, drukarki, używania polecenia sudo (czyli uruchamiania poleceń z prawami root), albo możliwość montowania patyków USB albo katalogów sieciowych⁵.

⁵ W sys. op. Linuks można montować katalogi sieciowe tak jak dyski twarde. Jest to możliwe dzięki temu, że sys. op. Linuks obsługuje masę popularnych protokołów sieciowych takich jak: **FTP**, **SMB** (znany z sys. **Windows**) oraz **NFS** (sieci sys. **Uniks**).

W praktyce dziś nie pracuje się na koncie root. Zamiast tego korzysta się z kont jakie należą do grupy sudo.

Polecenie sudo pozwala na wykonanie polecenia z prawem root-a. Najczęściej są to polecenia dotyczące instalacji prog. z sieciowych repozytoriów poleceniami apt.

sudo jest też używany do uruchamiania edytora tekstu w celu edycji systemowych plików konfiguracyjnych - z tej możliwości będziemy intensywnie korzystać.

1.3 Sys. Uprawnień w sys. op. Linuks

sys. op. Linuks na poziomie katalogów i plików rozróżnia 3 grupy uprawnień:

- Właściciel (nie wiadomo czemu po ang. jest to: user);
- Grupy do których należy właściciel (w j. ang.: group);
- Pozostali użytkownicy sys. (w j. ang.: others) należący do grup do jakich nie należy właściciel.

Każda z tych grup ma 3 stopnie dostępu:

- Odczyt (w j. ang.: read, w skrócie r);
- Zapis (w j. ang.: write, w skrócie w);
- Wykonanie (w j. ang.: execute, w skrócie x): dla plików oznacza możliwość uruchomienia takiego pliku (z prog. lub skryptem)

drwxrwxrwx

to flagi dostępu, które można ustawić dla kat. i plików. Jeśli wszystkie flagi rwx są ustawione tworzą one liczby, np.:

rwx	111	7	odczyt, zapis, uruchomienie
rw	110	6	odczyt, zapis
r	100	4	tylko odczyt
w	010	2	tylko zapis

x	001	1	tylko uruchomienie
---	-----	---	--------------------

Ustawiona flaga d oznacza, że to kat. w przeciwnym wypadku może to być plik, link symboliczny lub urządzenie.

Flaga wykonania ma inne znaczenie dla pliku i dla katalogu. W przypadku katalogu ustawiona flaga odczytu pozwala na odczyt zawartości katalogu. Jednak aby odczytać metadane plików w katalogu (wielkości plików i ich czasy) musi mieć on ustawioną flagę wykonania.

Katalog to plik z ustawioną flagą d. Format pliku opisujący zaw. katalogu jest ściśle zdefiniowany, a jego dane dostępne są za pośrednictwem sys. operacyjnego (w naszym przypadku to Linuks).

Jakie są prawa dostępu do pliku dowiesz się dzięki poleceniu ls, np:

```
$ ls -al /home
razem 28
drwxr-xr-x  4 root          root
4096 paź 11 18:28 .
drwxr-xr-x 20 root          root
4096 lip 18 2017 ..
drwx----- 57 energokoder energokoder
4096 sty 30 08:02 energokoder
drwx-----  2 root          root
16384 gru 19 2019 lost+found
```

Domyślnie prawa dostępu do katalogu domowego są takie:

drwxr-xr-x

Tak więc domyślnie katalog domowy (czytając od lewej):

- Jest katalogiem: flaga d;
- Właściciel może pobierać listę plików, dodawać i usuwać pliki oraz odczytywać ich metadane: rwx;
- Grupa może pobierać listę plików oraz odczytywać ich metadane: r-x;
- Pozostali może pobierać listę plików oraz odczytywać ich metadane: r-x;

Te domyślne prawa dostępu drwxr-xr-x są złe, bo umożliwiają pełen wgląd w katalog domowy innym

użytkownikom (nie tylko z grup do których należysz ale wszystkim w twoim sys. op. Linuks).⁶

Dlatego domyślne prawa należy zastrzyć. Jak widać ja już to zrobiłem bo prawa dostępu do mojego katalogu domowego (/home/energokoder) to drwx-----, czyli ja i root mamy pełen dostęp, a reszta żaden. Jak to zrobić podam niżej.

1.4 Piaskownice

Domyślny sys. praw dostępu w sys. op. Linuks powoduje, że prog. uruchomiony przez uż. ma pełen dostęp do jego kat. \$HOME. Nie trzeba być wielkim fatalistą by wyobrazić sobie wysyłanie listy moich prywatnych plików na nieznanne serwery gdzieś na Świecie. Jasne jest, że to samo może się stać z zawartością co ciekawszych spośród moich plików.

Piaskownica umożliwia wydzielenie elementów sys. operacyjnego, które są niezbędne do prawidłowego działania uruchamianej aplikacji. To znacznie zwiększa możliwości kontroli i świadomość tego co (w najgorszym przypadku) może zrobić podejrzany prog.

Brzmi to pięknie, ale:

Trzeba tworzyć brakujące profile piaskownicy dla nowych aplikacji.

Profile trzeba dostosowywać do zmieniających się aplikacji.

Profile trzeba dostosowywać do zmian wprowadzanych w własnej strukturze kat. \$HOME.

1.4.1 AppArmor - To Nie Piaskownica, Ale...

AppArmor nie jest piaskownicą, ale pozwala zastrzyć prawa dostępu do określonych plików dla konkretnych kat., plików i prog.

⁶ Jak zgaduję pretekstem dla którego takie prawa są nadawane katalogom domowym jest scenariusz w którym ktoś chce udostępnić jakiś podkatalog ze swojego katalogu domowego innym użytkownikom swojego komp. lub w sieci lokalnej. Tylko, że nikt w domu tego nie robi, bo to wymaga wiedzy o konfiguracji demonów sieciowych (FTP, SMB lub NFS albo innych), bo te demony odpowiadają za udostępnianie plików i katalogów.

Prawa dostępu określa dla każdej aplikacji specjalny plik profilu AppArmor. Dostępne są takie pliki z profilami dla popularnych prog. Jednak zamiast korzystać bezpośrednio z AppArmor ja proponuję używać piaskownicy Firejail. Firejail wew. używa AppArmor (lub SELinux na sys. z rodz. RedHat).

1.4.2 Piaskownice w Paczkach Snap i Flatpack

Paczki Snap i Flatpack powstały z powodu dużej il. niezależnych distr Linuksowych w celu robienia "jednej paczki dla wszystkich Linuksów". Jak to możliwe? Po prostu prog. rozprowadza się z paczką która zawiera dużą część bibl. sys. Z tym że paczki tworzy się na najstarszym wspieranym sys. op. Linux. To wystarcza by prog. działał na wielu distrach linuksowych.

1.4.2.1 Snap

"Odp. ChatGPT (OpenAI, model GPT-5.5) na pyt.

"Czy manifesty paczek snap i flatpack są jawne? Chodzi mi o to czy można się dowiedzieć do jakich zasobów chcą mieć one dostęp.", oraz:

"Kubuntu 20.04: Powiedz jakie mam możliwości kontroli piaskownicy w paczka Snap. Chodzi mi np. jak mogę kontrolować dostęp do wybranych podkatalogów w kat. domowym."

, w d. 2026-06-17, śro. Poniżej przytoczono wygenerowaną treść:

"Jak sprawdzić uprawnienia?

1. Interfejsy używane przez paczkę

snap connections firefox

Przykład:

<i>Interface</i>	<i>Plug</i>
<i>home</i>	<i>firefox</i>
<i>network</i>	<i>firefox</i>
<i>camera</i>	<i>firefox</i>
<i>audio-record</i>	<i>firefox</i>
<i>removable-media</i>	<i>firefox</i>

2. Deklaracje bezpieczeństwa

snap debug sandbox-features firefox

Włączanie i wyłączanie interfejsów

Przykład:

```
sudo snap disconnect firefox:camera
```

lub

```
sudo snap connect firefox:camera
```

Możesz więc odebrać dostęp do:

kamery,

mikrofonu,

urządzeń USB,

nośników wymiennych,

Bluetooth,

drukarek itd.

"

1.4.2.2 Flatpack

"Odp. ChatGPT (OpenAI, model GPT-5.5) na pyt.

"Czy manifesty paczek snap i flatpack są jawne? Chodzi mi o to czy można się dowiedzieć do jakich zasobów chcą mieć one dostęp.", oraz:

"Kubuntu 20.04: Powiedz jakie mam możliwości kontroli piaskownicy w paczka Snap. Chodzi mi np. jak mogę kontrolować dostęp do wybranych podkatalogów w kat. domowym."

, w d. 2026-06-17, śro. Poniżej przytoczono wygenerowaną treść:

Jak sprawdzić już zainstalowaną aplikację?

```
flatpak info --show-permissions  
org.mozilla.firefox
```

Przykład:

```
[Context]  
shared=network;  
sockets=x11;wayland;  
devices=dri;  
filesystems=home;
```

Jeszcze dokładniej

```
flatpak info --show-metadata  
org.mozilla.firefox
```

Flatpak pozwala użytkownikowi robić rzeczy, których Snap praktycznie nie umożliwia:

```
flatpak override  
--filesystem=~/.Dokumenty  
org.mozilla.firefox  
flatpak override --nofilesystem=home  
org.mozilla.firefox
```

czyli:

dostęp tylko do wybranego katalogu,

zakaz dostępu do całego \$HOME,

dodawanie i odbieranie uprawnień bez rekompilacji pakietu.

"

1.4.3 AppImage

To popularne paczki z prog. które nie wymagają instalacji i działają w trybie: 1 paczka to 1 aplikacja. Dobrym rozw. jest użycie piaskownicy firejail w celu ograniczenia prog. z paczek AppImage dostępu do zasobów sys. op. Linuks. Jak to zrobić pokażę w roz. Paczki AppImage.

Dziwną wadą paczek AppImage jest konieczność montowania zaw. paczki do sys. plików przy każdym uruchomieniu prog. I to w sytuacji gdy jest to b. wolne, bo przed zamontowaniem paczki należy ją rozpakować i to mimo że paczkę montuje się w trybie tylko do odczytu. Dlatego są lagi przy uruchamianiu prog. z paczki AppImage.

1.4.4 Piaskownica Firejail

Jest to piaskownica ograniczająca prog. dostęp do zasobów sys. op., do plików użytkownika i do Internetu. Na chwilę obecną na sys. rodz. Ubuntu firejail może kontrolować prog. z paczek *.deb (a także AppImage).

Firejail nie zadziała z prog. instalowanymi z paczek Snap, ani Flatpack, ani AppImage, bo one nie tolerują dodatkowych piaskownic.

Firejail działa w oparciu o AppArmor lub SELinux. Ma własny format plików z profilami jakie definiują ograniczenia uruchamianych prog.

Firejail wymaga konfiguracji sys. op. Linuks oraz konfiguracji katalogu użytkownika.

Konfiguracja sys. polega na utworzeniu linków symbolicznych w kat. /usr/local/bin z nazwami prog. jakie mają działać w piaskownicy firejail. Wszystkie te linki wskazują na /usr/bin/firejail .

Trik polega na tym, że jak wpisuje się skrócone polecenie (bez pełnej ścieżki), to prog. umieszczone "/usr/local/bin" mają priorytet nad tymi z "/usr/bin" (bez cudzo-słówów).

Konfiguracja katalogu użytkownika polega na modyfikacji plików "*.desktop" (i paru innych) tak by używały one skróconych poleceń, czyli bez ścieżki /usr/bin.

W katalogu /etc/firejail znajdują się profile prog.

Czasem zdarza się też że profile są nie aktualne i nie działają prog. do jakich są one przypisane. Zdarza się, że do nowych prog. nie ma profili. Ale jest na to sposób: repozytorium kodu źródłowego firejail na github.com !

<https://github.com/netblue30/firejail/tree/master/etc/profile-a-l>

<https://github.com/netblue30/firejail/tree/master/etc/profile-m-z>

Na tych stronach należy szukać aktualnych i brakujących profili. Należy je po prostu ściągnąć na dysk i skopiować do podanego wyżej katalogu.

Jednak nawet gdy nie ma profili dla danego prog., a jest potrzeba by go jakoś ograniczyć, to można bardzo łatwo stworzyć odpowiedni profil firejail. Niżej pokażę jak to zrobić.

1.4.5 Porównanie Piaskownic

"Odp. ChatGPT (OpenAI, model GPT-5.5) na pyt. "Kubuntu 20.04: Powiedz jakie mam możliwości kontroli piaskownicy w paczka Snap. Chodzi mi np. jak mogę kontrolować dostęp do wybranych podkatalogów w kat. domowym." w d. 2026-06-17, śro. Poniżej przytoczono wygenerowaną treść (fragment):

Możliwość	Snap	Flatpak	Firejail
Wyłączyć kamerę	✓	✓	✓
Wyłączyć mikrofon	✓	✓	✓
Odebrać cały \$HOME	✓	✓	✓
Dać dostęp tylko do ~/Dokumenty	✗	✓	✓
Zablokować	✗	✓	✓

Możliwość	Snap	Flatpak	Firejail
~/Prywatne			
Zmieniać reguły jako zwykły użytkownik	Ograniczenie	✓	✓
Bardzo szczegółowa kontrola	✗	Średnia	✓

1.5 Zapory Sieciowe

Do kontroli ruchu sieciowego używa się specjalnego prog. ograniczającego ruch sieciowy: zapory sieciowej⁷. Aby omówić ścianę sieciową musimy przedstawić sieć Internet.

1.6 Co Jest Nie Tak z VPN?

VPN jest to tunelowanie ruchu w sieci lokalnej przez sieć publiczną. Jest to potrzebne dużym, wielooddziałowym firmom by spinać oddziałowe sieci lokalne w jedną dużą sieć lokalną.

Natomiast ludziom wmawia się, że usługi VPN mogą poprawić ich prywatność. Jednak jest to trudne, bo nie ma podstaw by wierzyć w dobrą wolę usługodawcy VPN. On normalnie ma obowiązek udzielać Policji historię poł. z ost. 90 dni. Obecnie policja na całym świecie ma umowy które pozwalają jej na uzyskanie tych danych z zagranicy.

Wydaje się, że jedynym sensownym użyciem VPN było by skorzystanie z usług firmy z kraju neutralnego. Ale bez większych nadziei na 100% poufność. Lista krajów neutralnych wygenerowana przez ChatGPT (OpenAI, model GPT-5.5) w d. 2026-06-09, wto. Poniżej przytoczono wygenerowaną treść:

"Andora, Austria, Irlandia, Kostaryka, Liechtenstein, Malta, Mołdawia, Monako (neutralność ograniczona przez związki z Francją), Mongolia., San Marino, Serbia, Szwajcaria, Turkmenistan, Watykan."

Należy przy tym wiedzieć, że są dostępne listy adresów IP wszystkich firm świadczących usługi VPN. Tak, że część serwerów odrzuca poł. z tych adresów (np. news.chmruka.net).

⁷ W j. ang. firewall

1.7 Co Jest Nie Tak z Siecią Tor?

Sieć Tor działa w ten sposób, że klient się z nią łączy, jego zapytanie przechodzi przez sieć serwerów Tor i wychodzi w zupełnie innym miejscu świata jako zapytanie zupełnie innego komputera w sieci Internet (inne IP).

Nie można opłacić usługi dostępu do sieci Tor, jednak można wpłacać darowizny.

Należy przy tym wiedzieć, że są dostępne listy adresów IP wszystkich serwerów sieci Tor. Tak, że część serwerów odrzuca poł. z tych adresów (np. google.com i news.chmruka.net).

2 Budowa Sieci Internet

Cała sieć Internet (czyli ziemaska komputerowa sieć globalna) działa dzięki komputerom z sys. rodziny Unixs (w tym sys. op. Linuks).

Internet został stworzony jako sieć dla sys. op. Unixs podobnie jak język C został stworzony do ich zaprogramowania.

2.1 Struktura Sieci Internet

Obecnie sieć Internet jest podzielona na 3 obszary: sieć lokalna, Internet IPv4 i Internet IPv6. Bezpośrednia komunikacja między tymi sieciami jest niemożliwa. Ale istnieją usługi pośredniczące umożliwiające wymianę danych między tymi sieciami.

Sieć IPv4 wykorzystuje liczby 32 bitowe do numerowania urządzeń w tej sieci. Czyli może ich być $4G = 4 \cdot 1024 \cdot 1024 \cdot 1024$.

Sieć IPv6 wykorzystuje liczby 128 bitowe do numerowania urządzeń sieciowych. Czyli może być ich $4G \cdot 4G \cdot 4G \cdot 4G$.

Ilość adresów w IPv6 jest absurdalnie wielka, a same adresy nie są możliwe do zapamiętania przez człowieka.

2.2 Protokoły w Sieci Internet

2.2.1 Protokół IP⁸

IP jest protokołem bezpołączeniowym, przesyłającym paczki danych między punktami w sieci Internet. IP nie przejmuje się zagubionymi pakietami. W wersji IPv4 ma sumę kontrolną, a w wersji IPv6 jej nie ma. Wynika to z wiary w znaczną poprawę jakości kabli sieciowych od lat 70. XXw (wtedy powstawał protokół IPv4).

Z protokołu IP nie korzysta się bezpośrednio. Jest on używany do przenoszenia pakietów protokołów UDP i TCP.

2.2.2 Protokół UDP⁹

Protokół UDP jest przesyłany paczkami IP. UDP jest protokołem bezpołączeniowym. UDP dodaje informacje o numerze portu. UDP nie gwarantuje kolejności ani poprawności przesyłania pakietów.

Z UDP korzysta się do implementacji usług sieciowych w których wydajność jest ważniejsza niż poprawność. Są to usługi typu RIP (trasowanie pakietów w Internecie), DNS (mapowanie nazw domenowych na adresy IP), NTP (synchronizowanie czasu z zegarem atomowym), DHCP (automatyczne przydzielanie adresów IP w sieciach lokalnych), strumieniowanie dźwięku i filmów w sieci Internet.

2.2.3 Protokół TCP¹⁰

TCP jest przesyłany paczkami IP. TCP jest protokołem połączeniowym. TCP dodaje informacje o numerze portu. TCP gwarantuje prawidłową kolejność pakietów i ich poprawność¹¹.

Najbardziej widocznym zastosowaniem protokołu TCP jest protokół HTTP(S) do przesyłania plików HTML (czyli stron internetowych) oraz plików pomocniczych¹².

8 W j. ang.: Internet Protocol

9 W j. ang.: User Datagram Protocol. Jak widać zupełnie nonsensowna nazwa.

10 W j. ang.: Transmission Control Protocol. Jak widać zupełnie nonsensowna nazwa.

11 W razie potrzeby ponawia transmisję uszkodzonego lub utraconego pakietu.

12 Te pliki pomocnicze, to: skrypty **Jawa Z Krypt**, style **CSS**, obrazy, muzyka i filmy.

2.2.4 Porty w UDP i w TCP

Domony (czyli wg Micro\$lop usługi) sieciowe współdzielą jedną kartę sieciową w ten sposób, że rejestrują się na jednym (lub więcej - tak jak np. w przypadku Samby) z dostępnych 65535 portów (osobno dla UDP i TCP bo są one rozdzielone).

W przypadku stosowania zapory sieciowej serwer musi odblokować dany port UDP lub TCP, bo w przeciwnym wypadku demon nie będzie w stanie przyjmować połą.

Typowa sesja SSH, tak została opisana przez ChatGPT (OpenAI, model GPT-5.5) w d. 2026-06-11, czw. Poniżej przytoczono wygenerowaną treść:

1. "Serwer SSH (sshd) nasłuchuje na porcie 22.
2. Klient X otwiera u siebie jakiś losowy port lokalny, np. 54321.
3. Klient X nawiązuje połączenie z serwerem Y na porcie 22.
4. Serwer Y akceptuje połączenie. Powstaje nowe gniazdo opisane przez czwórkę:
X:54321 <-> Y:22
5. Jednocześnie sshd nadal nasłuchuje na porcie 22 i może przyjmować kolejne połączenia.
6. Cała sesja SSH odbywa się przez to samo połączenie TCP:
X:54321 <-> Y:22
7. Po zakończeniu sesji połączenie jest zamykane."

2.3 Sieć Lokalna

Sieć lokalną fizycznie tworzy router z portami LAN (kable) i antenami WLAN (fale radiowe). Sieć ta wykorzystuje specjalnie zarezerwowane adresy IPv4¹³ lub/i IPv6:

Wymienię tu pulę adresów prywatnych przeznaczonych dla prywatnych sieci IPv4 i IPv6:

¹³ Jeśli chodzi o prywatne adresy **IPv4**, to stanowią one relikty dawnych czasów gdy wszystkie adresy **IPv4** były podzielone na klasy.

IP	Sieć	Maska sieci	Maks. liczba kompów
v4	10.0.0.0 – 10.255.255.255	255.0.0.0	24 bity = 16M
v4	172.16.0.0 – 172.31.255.255	255.240.0.0	20 bitów = 1M
v4	192.168.0.0 – 192.168.255.255	255.255.0.0	16 bitów = 64K
v6	fd00::/8		64 bity = 4G* 4G

Komp. może należeć do wielu sieci lokalnych jednocześnie oraz może jednocześnie mieć wiele adresów IP¹⁴ zarówno lokalnych jak i publicznych.

Np. sprytny tel. może mieć publiczny adres IP przydzielony przez operatora tel. radiowej (LTE), a dodatkowo może być połączony w lokalnej sieci radiowej (WiFi) i mieć przydzielony adres IP w tej sieci lokalnej. W tym przypadku są to 2 różne karty sieciowe. Jednak nawet jedna karta sieciowa może mieć wiele adresów IP.

2.4 NAT Czyli Lokalna Brama Do Globalnej Sieci Internet

By dostać dostęp do globalnej sieci komputerowej (czyli do sieci Internet) potrzebny jest komp. z funkcją NAT. Tą funkcję pełni router w którym działa sys. op. Linuks. On jest pośrednikiem który „udaje”, że to on wysyła zapytania do serwerów jakie wywołują, a odebrane dane przekazuje do mojego kompa w sieci lokalnej.

Mówi się, że „router tuneluje połączenia z komp. z sieci lokalnej do sieci Internet”.

Aby w ogóle się móc połączyć z siecią Internet trzeba mieć włączoną na routerze usługę DHCP lub samodzielnie poprzydzielać statyczne adresy IP urządzeniom w sieci lokalnej. Czasem ręczne przydzielanie statycznych adresów IP jest konieczne: np. w przypadku serwerów i drukarek. Można to zrobić na 2 sposoby:

1. Ustawić ręcznie adresy IP na każdym z komp. w sieci lokalnej;
2. W routerze, w konfiguracji DHCP zdefiniować jakie adresy IP przydzielać adresom MAC (adresy MAC to 48bit. identyfikatory fizycznych

¹⁴ I to na tej samej karcie sieciowej.

urządzeń sieciowych – są używane w warstwie fizycznej modelu sieciowego ISO-OSI).

Uważaj, by ustawić w routerze zakres adresów używanych przez DHCP, tak by nie kolidował on z adresami statycznymi IP jakie nadałeś swoim urządzeniom.

Znacznie lepiej samemu ponadawać adresy IP swoim urządzeniom w sieci, gdyż w takim przypadku mogą bez zastanawiania się łączyć się z własnymi kompami i mam przynajmniej częściową kontrolę nad symboliką numerów IP.

2.5 Sieć Globalna, Czyli Internet

W sieci globalnej IPv4 jest podzbiorem IPv6.

W praktyce komp. w sieci Internet dzielą się na 3 grupy:

- Routery: one spinają całą sieć. One tworzą graf z cyklami¹⁵. To powoduje, że sieć jest odporna na awarie. Bo gdy zostanie przerwana jedna linia to ruch może zostać skierowany inną;
- Serwery: one świadczą usługi z jakich się najczęściej korzysta. One są najbardziej widoczne dla ludzi;
- Pozostałe: Mogą to być zwykłe stacje robocze albo np. sprytny tel. z dostępem do sieci Internet. Mogą to też być proste mikrokontrolery z czujnikami lub różne sterowniki.

Praktycznie cały Internet jest oparty o kable. Tylko punkty dostępowe tej sieci bywają bezprzewodowe. Czyli to, że wysyłasz list el. z komp. w sieci lokalnej przez WiFi, albo ze sprytnego tel., to i tak przy najbliższej okazji jest on pchany w kabel i leci w ziemi do odbiorcy. I nie ma tu znaczenia, że ten odbiorca też może mieć WiFi czy sprytny tel. połączone z siecią radiowo.

Niektórzy nawet dziś wierzą, że tel. komórkowy wykorzystuje satelity. Ale to jest całkowity nonsens i głupota¹⁶.

15 Oczywiście dba się o to by pakiety nie krążyły w cyklach, tylko by wędrowały po ścieżkach w tym grafie.

16 Są specjalne terminale udostępniające **Internet** przez sieć sztucznych satelit ziemskich (obecnie chyba wyłącznie są to sieci stara - **Iridium** i nowa - **Starlink**). Ale to odpowiednio kosztuje i jest jasno

2.6 Nazwy Domen a IP

Na co dzień w sieci Internet posługujemy się takimi nazwami jak onet.pl albo wp.pl . Są to domenowe nazwy serwerów. Są one wył. dla naszej ludzkiej wygody. Każdorazowo gdy trzeba coś wysłać do takiego serwera przeglądarka korzysta z usługi DNS (która oparta jest o protokół bezpołączeniowy UDP) tłumaczy je na faktyczne adresy IP i dalej komunikacja odbywa się tak jak to wcześniej opisywałem.

Należy zwrócić uwagę że istnieje sztuczka programowa pozwalająca na obsługę wielu domen przez serwer o jednym IP,

cytat: „To się nazywa "virtual hosting". Możliwy dzięki HTTP/1.1: kiedy przeglądarka łączy się z serwerem HTTP, wysła mu nie tylko prośbę o daną ścieżkę (np. "GET /strona.html"), ale również pole "Host" w którym wpisuje nazwę (FQDN) serwera (np. "Host: energokod.gda.pl"). Serwer HTTP może mieć milion domen na jednym IP, aby wybrać, którą stronę odpowiedzieć sprawdza po prostu pole "Host"."

źródło: grupa dyskusyjna pl.comp.sieci, temat wątku „Jak działa hosting w którym wykupuje się sam serwer i domenę, bez IP?”, odp. z d. 2025-08-15, godz. 20:33, aut. Mateusz Viste.

3 Wybór Modelu Bezpieczeństwa w Pracy z Sys. Op. Linuks

3.1 Domowa Stacja Robocza - Sys. Online

Założenia tego sys.:

1. Instalacja na stacji roboczej wybranego distro;
2. Całkowita blokada w UFW poł. Przychodzących;

podane, że to usługa satelitarna.

3. Używanie piaskownicy firejail do kontroli prog.: Brave (przeglądarki), Thunderbird (klienta pocztowego), Elinks (przeglądarki tekstowej), wget (pobieranie w konsoli plików z internetu).

Użycie sieci Internet:

B. dobrym rozw. jest użycie czytnika kanałów RSS newsboat i specjalnie dla niego przygotowaną tekstową przeglądarką tekstową elinks (z wył. j. Java Skrypt i bez Cookies). Natomiast do reszty zastosowań można po starym używać normalnej przeglądarki takiej jak Brave.

3.2 Firmowa Stacja Robocza - Sys. Offline z Lustrzanym Repo w Sieci Lokalnej

Mimo, że mało kto o tym mówi szpiegostwo sieciowe obecnie kwitnie. I wcale nie jest oparte na włamywaniu - bo najczęściej szpiegują programy i urządzenia uruchamiane w sieciach lokalnych.

Dlatego we wszystkich polskich firmach w których są działy B+R (badawczo-rozwojowe) należy przyjąć reżim taki jak w WP (Wojsku Polskim) i całkowicie odciąć sieć lokalną od Internetu. Dodam, że w WP nie stosuje się też sieci Wi-Fi. Jednak niektóre proj. wymagają tego typu sieci. Aby załagodzić skutki pracy offline, można zafundować sobie "lokalne, lustrzane repo" z Canonical. Obecnie jest taka możliwość.

Utworzenie własnego, lokalnego repo używanego distro jest fajną opcją również dlatego, że dzięki temu można się zabezpieczyć przed psuciem distro w kol. aktualizacjach oraz przed wył. oficjalnego repo. Dla firmy lub nawet dla osoby pracującej taki serwerek to nieduży wydatek. Jednak trzeba wiedzieć o wadach tego rozwiązania:

1. Aktualizacja lustrzanego repo wymaga dodatkowego serwera: wynika to z faktu, że nie można wykluczyć wysyłania na serwery źródłowe jakichś archiwalnych danych z serwerów lustrzanych. Dlatego pozostaje duplikacja fizycznego serwera, lub kasowanie i instalacja całego repo od zera. Można też by się bawić w kasowanie niektórych polików, ale słabym p. jest

to, że nawet jak dziś pokasujesz wszystko co trzeba, to jutro będzie to za mało.

2. Firmowe repo z paczkami deb: Zrobienie lustrzanych kopi wszystkich firmowych repo z paczkami deb (z poza Canonical) było by istotnym udogodnieniem.

Na ten moment nie wiem jak można by zrobić lustrzane kopie wszystkich firmowych repo z paczkami deb. A to było by w pełni komfortowym rozw.

Szczegóły: W 2022r. dowiedziałem się o istnieniu skryptu [get-deb.sh](https://github.com/lepture/get-deb.sh). Służy on do instalacji paczek deb z firmowych repo. Nie znam się na tworzeniu własnych repo, ale po rzucie oka na kod skryptu widać, że konfiguracja tych repo to coś zupełnie innego niż konfiguracja domyślnego repo instalowanego z sys. Ubuntu czy Debian.

3. Paczki Snap: Sys. tworzenia i dystrybucji paczek Snap stworzył Canonical (wydawca distro rodziny Ubuntu). Głównym celem jego stworzenia było zwiększenie przenośności oprogramowania (przez włączanie do paczki części wymaganych bibl.) (to zwiększenie przenośności chciano najprawdopodobniej zapewnić paczkom na sprytny tel. jaki Canonical kiedyś chciało opracować) oraz poprawa bezpieczeństwa przez wbudowaną piaskownicę.

Nie można wykonać lustrzanej kopii repo z paczkami Snap.

Można jednak pobierać pojedyncze paczki Snap z sieci Internet i instalować na chronionej stacji roboczej. Jednak trzeba mieć na uwadze, że interesujące paczki Snap mogą wymagać innych paczek Snap;

4. Paczki Flatpack: Sys. tworzenia i dystrybucji paczek Flatpack stworzył Red Hat jako konkurencję dla paczek Snap.

Nie znalazłem w sieci Internet żadnych informacji na temat możliwości tworzenia lustrzanych repo z paczkami Flatpack.

Paczki Flatpack mogą mieć 2 formy: „zwykłą” oraz "Single-file bundles". Tylko ta druga postać pozwala na dystrybucję i instalację bez dostępu do sieci Internet. „Zwykłe” paczki Flat-

pack też można przekonwertować do "Single-file bundles". Jednak prawdopodobnie może to zrobić tylko wydawca prog. Moje podejrzenie wynika z faktu stosowania podpisów cyfrowych w tych paczkach.

5. Paczki AppImage: Sys. tworzenia paczek AppImage stworzył Niemiec Peter Simon o pseudonimie Probono¹⁷. W porównaniu do sys. Snap i Flatpack AppImage wypada rewelacyjnie: Prosta koncepcja: jedna paczka to jeden prog.; Prosta, tradycyjna koncepcja tworzenia paczek; Podobna odporność paczek na zmiany w sys. op. (przez włączanie do paczki części wymaganych bibl.).

Nie znalazłem w sieci Internet żadnych informacji na temat możliwości tworzenia lustrzanych repo z paczkami AppImage.

Założenia tego sys.:

1. Masz łącze światłowodowe (tak rurę do sieci Internet). W przeciwnym wypadku możesz się nie doczekać na pobranie kopii repo.
2. Na serwer wystarczył by stary komp stacjonarny. Jednak problem jest taki, że stare kompy mają stare procki które zużywają dużo energii nawet w stanie bezczynności¹⁸. Można to zignorować jeśli po pobraniu kopii lustrzanej repo możesz sobie pozwolić na wł. serwera tylko gdy to niezbędne.

Serwer musi mieć dysk w macierzy RAID.

3. Konfiguracja sieci lokalnej tak by mogły w niej działać serwer z lustrzaną kopią repo Ubuntu i stacja robocza na której się pracuje;

Konfiguracja serwera jest ROZDZIALE PONIŻEJ.

Użycie sieci Internet:

4. Sieć należy przeglądać przeglądarką w sprytnym tel. Potrzebne pliki przegrywać na patyk USB i przenosić na "firmową stację roboczą".

¹⁷ W j. łac. "Pro bono publico " - w j. pol.: Dla dobra publicznego (bez zapłaty).

¹⁸ po ang. idle

4 Przygotowanie Do Instalacji Sys. Op. Linuks

Aby w ogóle mieć sys. op. Linuks musisz pobrać najpierw prog. instalacyjny w postaci obrazu ISO. Ten plik następnie trzeba zweryfikować i nagrać na patyk USB. Podam tu instrukcje jak to zrobić:

4.1 Jaką Dystrybucję Wybrać?

4.1.1 Smaki Ubuntu

Pomysł na ten roz. podsunął mi "głos w szumach" jaki przedstawia się agent "Łukasz Niewiadomski" ze SP nr 3 w Pruszczu Gd. z kl. 3A.

Ten roz. w całości został wygenerowany przez ChatGPT (OpenAI, model GPT-5.5) w d. 2026-06-13, sob, po zadaniu pyt.:

"Podaj oficjalne i nieoficjalne smaki Ubuntu oraz ich najważniejsze cechy.";

Poniżej przytoczono wygenerowaną treść:

"Poniżej zestawienie najważniejszych odmian Ubuntu. Wszystkie korzystają z tych samych repozytoriów i jądra Linux, różnią się głównie środowiskiem graficznym i doбором programów. ([Ubuntu](#))

4.1.1.1 Oficjalne smaki Ubuntu

Smak	Środowisko	Najważniejsze cechy
Ubuntu	GNOME	Domyślna wersja Canonical, nowoczesny interfejs, dobre wsparcie sprzętu
Kubuntu	KDE Plasma	Bardzo konfigurowalne, przypomina Windows, bogaty zestaw aplikacji KDE
Xubuntu	Xfce	Lekki i stabilny, dobre dla starszych komputerów
Lubuntu	LXQt	Bardzo małe wymagania sprzętowe, szybki
Ubuntu MATE	MATE	Klasyczny wygląd GNOME 2, wygodny dla starszych użytkowników

Smak	Środowisko	Najważniejsze cechy
Ubuntu Budgie	Budgie	Elegancki i prosty interfejs
Ubuntu Cinnamon	Cinnamon	Wygląd podobny do Linux Mint, wygodny dla użytkowników Windows
Ubuntu Studio	KDE Plasma	Programy dla grafiki, audio i wideo, małe opóźnienia dźwięku
Edubuntu	GNOME	Pakiety edukacyjne dla szkół
Ubuntu Kylin	UKUI	Przeznaczony głównie dla rynku chińskiego
Ubuntu Unity	Unity	Powrót dawnego interfejsu Ubuntu 10.10-17.04

4.1.1.2 Popularne nieoficjalne smaki (remiksy)

Smak	Środowisko	Cechy
UbuntuDDE	Deepin	Bardzo atrakcyjny wizualnie, przypomina macOS
Ubuntu Sway	Sway	Menedżer kafelkowy zgodny z Waylandem
Ubuntu Web	/	System zorientowany na aplikacje webowe
Ubuntu Cinnamon Remix	Cinnamon	Poprzednik oficjalnego Ubuntu Cinnamon
Ubuntu Lumina	Lumina	Lekki pulpit rozwijany niezależnie od Qt/KDE
Ubuntu CE	GNOME	Wersja z aplikacjami chrześcijańskimi
UbuntuDDE Remix	Deepin	Jeden z najbardziej dopracowanych nieoficjalnych wariantów

4.1.1.3 Popularne nieoficjalne pochodne Ubuntu

Dystrybucja	Cechy charakterystyczne
Trisquel	100% wolne oprogramowanie, jądro Linux-libre, brak własnościowych sterowników i firmware, rekomendowana przez FSF
Linux Mint	Bardzo przyjazna dla użytkowników Windows, Cinnamon/MATE/Xfce
Pop!_OS	Rozwijana przez System76, dobra dla programistów i graczy
Zorin OS elementary OS	Interfejs przypominający Windows Wygląd inspirowany macOS

Dystrybucja	Cechy charakterystyczne
UbuntuDDE	Środowisko Deepin, atrakcyjny wygląd
KDE neon	Najnowsze KDE Plasma na bazie Ubuntu LTS
Nitrux	KDE Plasma z własnymi modyfikacjami
Peppermint OS	Lekki system z integracją aplikacji webowych

4.1.2 Który [Smak Ubuntu - przyp. JMJ] wybrać?

- **Dla początkujących** – Ubuntu lub Kubuntu.
- **Dla starszego sprzętu** – Lubuntu lub Xubuntu.
- **Dla osób przyzwyczajonych do Windows** – Kubuntu lub Ubuntu Cinnamon.
- **Dla zwolenników klasycznego GNOME 2** – Ubuntu MATE.
- **Dla grafików, muzyków i twórców wideo** – Ubuntu Studio.
- **Dla miłośników pięknego wyglądu** – Ubuntu Budgie lub UbuntuDDE.
- **Dla zaawansowanych użytkowników i programistów** – Ubuntu Sway.

Ponieważ z wcześniejszych rozmów wiem, że używasz Linuksa i programujesz w C/C++, szczególnie interesujące mogą być **Kubuntu** (wygodne dla Qt i KDE), **Xubuntu** (lekkość) oraz **Ubuntu MATE** (bardzo stabilne i klasyczne).

4.1.3 Oficjalne odmiany Ubuntu Server

Ten roz. w całości został wygenerowany przez ChatGPT (OpenAI, model GPT-5.5) w d. 2026-06-13, sob, po zadaniu pyt.:

"Podaj oficjalne i nieoficjalne smaki Ubuntu Serwer oraz ich najważniejsze cechy."

Poniżej przytoczono wygenerowaną treść:

W przypadku **Ubuntu Server** sytuacja jest trochę inna niż dla Ubuntu Desktop. Nie ma oficjalnych „smaków serwerowych” w sensie różnych środowisk graficznych. Istnieje jedna oficjalna dystrybucja **Ubuntu Server**, a wokół niej powstało wiele odmian i projektów specjalizowanych.

Odmiana	Najważniejsze cechy
Ubuntu Server	Uniwersalny serwer, pakiety DEB/APT, 5 lat wsparcia dla LTS
Ubuntu Minimal	Minimalna instalacja bez zbędnych pakietów
Ubuntu Cloud Images	Obrazy dla AWS, Azure, OpenStack itp.
Ubuntu Pro	Dłuższe wsparcie bezpieczeństwa (ESM), zgodność dla firm
Ubuntu Core	System dla IoT i urządzeń wbudowanych, wyłącznie Snap, transakcyjne aktualizacje
MicroCloud	Budowa prywatnych chmur z LXDE i MicroCeph
MAAS + Ubuntu Server	Zarządzanie dużą liczbą serwerów fizycznych
Charmed OpenStack	Platforma chmury prywatnej
JeOS (historyczny)	Bardzo mały system dla maszyn wirtualnych, zastąpiony przez Ubuntu Core

4.1.3.1 Popularne nieoficjalne odmiany i pochodne

Dystrybucja	Cechy
Trisquel Server	100% wolne oprogramowanie, Linux-libre
Linux Mint Debian Edition Server	Nie istnieje jako osobna wersja, ale Mint bywa stosowany po doinstalowaniu usług
TurnKey Linux	Gotowe appliance'y (Nextcloud, GitLab, WordPress, PostgreSQL itd.)
Proxmox VE	Wirtualizacja KVM + kontenery LXC, baza Debian/Ubuntu
NethServer	Łatwe zarządzanie małymi serwerami firmowymi
Zentyal Server	Serwer dla małych firm, odpowiednik Windows Server
ClearOS	Brama internetowa i serwer usług sieciowych
Ubuntu Appliance	Gotowe obrazy dla Raspberry Pi i serwerów domowych
FreedomBox	Serwer prywatności i usług domowych
YunoHost	Prosta platforma do samodzielnego hostingu usług

4.1.3.2 Projekty oparte bezpośrednio na Ubuntu Server

- **Kubuntu Focus Server**

- **Pop!_OS Server** (nieformalnie, przez instalację usług)
- **Ubuntu Appliance Nextcloud**
- **Ubuntu Appliance Mosquitto**
- **Ubuntu Appliance AdGuard Home**
- **Ubuntu Appliance Home Assistant**

4.1.3.3 Dla jakich zastosowań?

Zastosowanie	Polecana odmiana
Serwer WWW, SSH, Samba, NFS	Ubuntu Server
Domowy NAS	Ubuntu Server + Cockpit lub TurnKey File Server
Wirtualizacja	Proxmox VE
Chmura prywatna	MicroCloud lub OpenStack
Raspberry Pi	Ubuntu Server ARM lub Ubuntu Appliance
W pełni wolne oprogramowanie	Trisquel Server
Mała firma	Zentyal lub NethServer
IoT	Ubuntu Core
Gotowe usługi bez konfiguracji	TurnKey Linux

Najbliższym odpowiednikiem „smaków Ubuntu Server” są właśnie **TurnKey Linux**, **Ubuntu Appliance**, **Trisquel Server**, **Zentyal**, **NethServer** czy **FreedomBox** — czyli dystrybucje lub obrazy wyspecjalizowane do konkretnych zadań, zamiast różnych środowisk graficznych."

4.1.4 Wybierz Dystrybucję Typu LTS

Pozytywnym efektem wiad. pt. [GNU Linux nie jest stabilnym systemem - prawdziwy dowód](#), którą opublikowałem na grupie dyskusyjnej pl.comp.os.linux w d. 2011-12-17, sob. było pojawienie się wkrótce dystrybucji sys. op. Linuks o wsparciu przedłużonym do 10 i więcej lat. W praktyce na wydaniach distro Ubuntu LTS można w spokoju pracować przez długie lata. Jest to nie tylko konieczne dla biznesu, ale też dla wszystkich profesjonalistów, którzy tworzą własne prog. i skrypty. Teoretycznie distro LTS pozwala uniknąć ciągłego szarpania się z niekompatybilnymi zmianami w bibl. i w poleceniach konsoli.

4.1.5 Są Dystrybucje Bez Zamkniętych Pakietów - Ale Czy Warto Je Instalować?

Fundacja FSF rozróżnia całkowicie wolne dystrybucje od tych co dodają pakiety z zamkniętym oprogramowaniem¹⁹. Otwarte dystrybucje są wymienione na stronie: <https://www.gnu.org/distros/free-distros.html>. Natomiast uzasadnienie dla których inne popularne dystrybucje są uznawane za nie w pełni wolne jest na stronie: <https://www.gnu.org/distros/common-distros.html>.

Zamknięte oprogramowanie dotyczy nawet samego rdzenia sys. op. Linuks - do jego pakietów pakowane są np. binarne mikrokody.

Te mikrokody nabierają praktycznego znaczenia w momencie gdy trzeba skorzystać z urządzeń które ich wymagają. Np. zdarzyło mi się, że nowo kupiony tuner TV ich wymagał, co spowodowało konieczność powrotu z w pełni wolnej i otwartej dystrybucji Triksel na Kubuntu (ale ten tuner i tak mi nie zadziałał, bo aktywna antena pokojowa go spaliła).

4.2 Jak Prawidłowo Zainstalować Sys. Op. Linuks Mając Tylko Skompromitowany Sys. Komp.

Jeśli do tej pory nie przejmowałeś się zabezpieczeniem swojego sys. komp., to możesz śmiało założyć, że jest on spenetrowany. Wtedy pojawia się pytanie: czy mając taki skompromitowany sys. można postawić nowy zabezpieczony? Tak! Jednak trzeba postępować w sposób logiczny eliminując możliwość modyfikacji instalacji dystrybucji przez intruza. To oznacza:

1. Ściągnięcie instalacji dystrybucji sys. op. Linuks (pliku ISO);
2. Ściągnięcie pliku z sumami kontrolnymi (koniecznymi do weryfikacji oryginalności pliku ISO);
3. Odłączenie komp. od sieci;

¹⁹ Zamknięte oprogramowanie to oprogramowanie do którego kody źródłowe nie są dostępne.

4. Spr. obrazu ISO;
5. Nagranie obrazu ISO na USB;
6. Uruchomić komp. z USB w celu instalacji sys. op. Linuks.

Jak to wszystko zrobić podaję poniżej.

4.3 Pobieranie Obrazu instalacji Sys. Op. Linuks

By pobrać instalkę Ubuntu, np.:

```
wget
https://releases.ubuntu.com/resolute/ubuntu-26.04-desktop-amd64.iso
```

Oczywiście, zamiast tej powyższej, powinieneś pobrać aktualnie najnowsze wersje twojej ulubionej dystrybucji sys. op. Linuks opartej na sys. Ubuntu.

4.3.1 Pobranie Sum Kontrolnych

Generalnie sumy kontrolne są publikowane na serwerach w tych samych katalogach w jakich są pliki obrazów ISO. Czasem trzeba trochę poklikać na stronie dystrybucji by do nich dotrzeć. W powyższym przypadku sumy kontrolne znajdują się w pliku:

```
wget
https://releases.ubuntu.com/resolute/SHA256SUMS
```

4.3.2 Odłącz Komp. Od Sieci

Bardzo ważne jest by nikt nawet teoretycznie nie mógł zmodyfikować pobranego pliku ISO po jego weryfikacji ani po nagraniu na USB.

W RAZIE GDYŚ POTRZEBOWAŁ JAKICHŚ PROG. JAKIE TRZEBA POBRAĆ Z SIECI INTERNET W CELU SPR. I NAGRANIA PLIKU ISO NA USB, INSTALACJĘ sys. op. Linuks POWINIENEŚ ZACZAĆ OD TEGO MIEJSCA.

4.3.3 Spr. Pobranego Obrazu

Po pobraniu obrazu należy go spr.:

```
sha256sum ubuntu-26.04-desktop-amd64.iso
```

I porównać wzrokowo wynik z zawartością pliku z sumami kontrolnymi (w tym przypadku z pobranego wcześniej pliku **SHA256SUMS**).

4.3.4 Nagrywanie Obrazu

Obraz z sys. należy nagrać na pamięć USB. Musi ona mieć co najmniej 8GB.

Tu znowu musimy się trochę zastanowić. Czy użyć choinkowego i idiotoodpornego Etcher-a? Czy może się wysilić, zaryzykować i użyć dd?

Odpowiedź to: dd.

Dlatego, że jest to prog. z otwartymi źródłami w które (teoretycznie) patrzyło wiele osób pracujących przy różnych wielu dystrybucjach sys. op. Linuks. Natomiast nikt nie wie co tak na prawdę siedzi w prawie 200MB paczce Etcher. Dlatego dla świętego spokoju lepiej użyć dd.

Natomiast jeśli do tej pory używałeś Windows to [inst-ubun-desk-www] zaleca nagranie obrazu ISO na patyk USB za pomocą prog. <https://rufus.ie/pl>.

4.3.4.1 Rozpoznawanie Napędów w Sys. Op. Linuks

W sys. op. Linuks początkujący mogą czuć się zakłopotani jak rozpoznać to gdzie jest podpięty ich patyk USB (na który trzeba nagrać obraz ISO z instalką).

W sys. op. Linuks standardowo patyki USB pojawiają się jako pliki w katalogu /dev w momencie gdy je wtykasz do portu USB. Mają one nazwy sd* gdzie * to a, b, c itd.

Jednak w ten sam sposób są oznaczane są dyski SSD. Dlatego aby ustalić nazwę pamięci USB należy:

1. Wyjąć pamięć USB z portu USB (jeśli była włożona);
2. Użyć polecenia:

```
ls /dev/sd*
ls: nie ma dostępu do
'/dev/sd*': Nie ma takiego pliku
ani katalogu
```

Ja akurat mam inny dysk niż SSD, tak więc u mnie to polecenie zwraca błąd.

3. Wpiąć pamięć USB i ponownie wywołać

```
ls /dev/sd*
/dev/sda /dev/sda1
```

4. Wtedy wpis którego wcześniej nie było będzie nazwą naszej pamięci USB.

Napędem (tu: pamięć USB) jest tylko wpis bez cyfry. Cyfry po nazwie dysku oznaczają partycje jakie na nim się znajdują i może być ich wiele. Czyli w powyższym przykładzie pamięcią USB jest /dev/sda i ma on jedną jedyną partycję /dev/sda1 .

4.3.4.2 Zapis Obrazu Na Patyk USB

JAK POMYLISZ NAPĘD SSD Z USB TO MOŻESZ SOBIE WYMAZAĆ DYSK ZE STARYM SYS. OP. TAK WIĘC SPR. 2x CZY ZAPISUJESZ OBRAZ NA PAMIĘĆ USB.

```
dd if=./ubuntu-26.04-desktop-amd64.iso
of=/dev/sda bs=300M status=progress
```

Za if= podajesz ścieżkę do pliku ISO, of= to pamięć USB na którą zapisujemy obraz, bs= to wielkość pojedynczego kopiowanego pakietu, status=progress będzie informował o postępie kopiowania.

4.4 Uruchomienie Instalki

Instalację należy rozpocząć w trybie próbnego uruchomienia sys. op. Linuks²⁰. W tym trybie musimy przygotować się do instalacji przygotowując partycje i przygotowując silne hasło.

4.5 Partycjonowanie Dysku

Partycje na dysku to podział dysku na logiczne części. Każdą taką część definiuje się osobno i osobno na nich zakłada się sys. plików. Dopiero po podziale dysku na partycje i po założeniu na nich sys. plików można instalować sys. op.

Rozwój sys. plików ciągle trwa i wiąże się z nimi duże nadzieje głównie w zakresie bezpieczeństwa (szyfrowanie w locie, odporność na uszkodzenia nośnika, większa odporność na awarie zasilania) i wydajności (kompresja w locie).

Współczesne sys. op. Linuks oferują wygodne prog. do manipulacji partycjami np. w KDE „Zarządzanie partycjami”, a w Gnome gparted.

²⁰ W j. ang.: live mode

Proponuję przygotować następujące partycje:

Punkt montowania	Rozmiar	Typ	Przeznaczenie
Bios Grub	1MB	[BRAK] ²¹	Prog. rozruchowy Grub. Wymagana do uruchomienia sys. z dyskami GPT na starych komp. z BIOS.
/efi	300MB	Fat32 ²²	Firmware i prog. rozruchowy. Wymagana do uruchomienia sys. na nowych komp. z UEFI jaki jest następcą BIOS.
/boot	2GB ²³	Ext2	Pliki z obrazami rdzenia sys. op. Linuks. Wymagana do uruchomienia startych komp. z dużymi dyskami. Zabezpiecza przed zapelnieniem dysku przez zbyt dużo starych rdzeni sys. op. Linuks.
/tmp	20GB ²⁴	Ext2	Pliki tymczasowe (domyślnie do 10 dni ²⁵). Zabezpiecza przed zapelnieniem dysku przez zbyt duże pliki tymczasowe.

21 Powodem dla którego partycja Bios Grub nie ma typu jest to, że ona jest całkowicie kontrolowana przez Grub i sys. op. Linuks nic nie wie co na niej się dzieje.

22 Powodem dla którego partycja EFI ma typ Fat32 jest to, że jest to typ kompatybilny z sys. plików EFI.

23 Niektórzy zalecają wielkość partycji /boot na 100-300MB. Jednak to się nie sprawdza bo pliki rdzenia sys. op. Linuks mają prawie po 100MB (2021-02). Wydawcy dystrybucji sys. op. Linuks prawie co tydzień wydają nową wersję rdzenia. Normalnie powinni zostawiać tylko dwie wcześniejsze wersje (pierwszą opublikowaną i ostatnią działającą), jednak obecnie (2022-09) z nieznanym powodów zostawiają wiele starych wersji rdzenia. Stąd konieczne zabezpieczenie przed rozrostem katalogu /boot.

24 W poradnikach **WWW** podają by partycje **tmp** miały po 2GB. Ja jednak już się naciąłem na takim sknerstwie: instalator Qt korzysta z katalogu **tmp** i dla niego 2GB to za mało. Wtedy ratunkiem była

/var	20GB	Ext2	Pliki różne: w tym kat. /var/tmp (domyślnie do 30 dni), /var/log, /var/cache. Zabezpiecza przed zapelnieniem dysku przez zbyt duże pliki tymczasowe w kat. /var/tmp, /var/log i /var/cache.
/opt	20GB	Ext2	Pakiety z oprogramowaniem firm 3. Jak np. Google Chrome, albo sterowniki urządzeń drukująco-skanujących. Zabezpiecza przed zapelnieniem dysku przez zbyt duże pakiety nieznanym firm.
/usr/local	20GB	Ext2	Bibl. i prog. samodzielnie budowane i instalowane poleceniami: <pre>rm -fr ./budowa mkdir ./budowa cd ./budowa cmake .. make sudo make install cd ..</pre> Zabezpiecza przed zapelnieniem dysku przez zbyt duże prog. i bibl. instalowane przez użytkownika.
/	100GB	Ext2	Prog. i ustawienia sys. op.
/home	(reszta)	Ext4	Katalogi użytkowników.

instalacja „na raty”. 20GB ma też korzystną symbolikę: „20 giba bytów”.

```
25$ grep /tmp
/usr/lib/tmpfiles.d/tmp.conf
```

Powinien zwrócić:

```
q /tmp      1777 root root 10d
q /var/tmp  1777 root root 30d
```

Powodem dla którego partycje /, /boot, /opt, /usr/local, /tmp i /var mają typ EXT2 jest to, że:

1. EXT2 nie obsługuje transakcji przy zapisie danych²⁶;
2. Prawdopodobnie transakcje spowalniają zapis na dysk w sys. plikowych Ext3 i Ext4;
3. Na partycjach /, /boot, /opt i /usr/local normalnie nie dokonuje się zapisu;
4. Na partycji /tmp nie zapisuje się nic wartego ochrony transakcyjnej;
5. Jedyny problem jest z kat. /var/log który potencjalnie może utracić dane w wyniku zawieszenia sys. op. Linuks przez intruza.

Na partycji /home zalecam używać Ext4 gdyż ma on transakcje przy zapisie i jest nowszy od Ext3 (który też ma transakcje). Sys. plików serii Ext są oficjalnymi sys. plików dla sys. op. Linuks.

Partycji nigdy nie należy przesuwać, bo z nieznanych powodów ta operacja nigdy się nie udaje, bo trwa w nieskończoność. Jest tak nawet na komp. z dziesiątkami GB RAM. Prowadzi to do konieczności awaryjnego przerwania operacji przesuwania partycji w wyniku czego dochodzi do ich zniszczenia i utraty danych.

Jednak, cytat:

"==> I tu mam małą ciekawostkę: spotkałem się z tym problemem, ale tylko na prawdziwej maszynie! Na VM

problem NIE występuje!. Zawsze używałem do przesuwania partycji programu Gparted. I to co opisałeś zawsze występuje na prawdziwej maszynie, a na VM nie. Zawsze oczywiście takie operację wykonywałem spoza uruchomionego systemu na dysku twardym (zarówno prawdziwym jak i wirtualnym) za pomocą dystrybucji typu Live CD (konkretnie Rescuezilla) a partycje modyfikowane nie były zamontowane."

, źródło: list el. pt. "Komentarz do monografii „Zabezp. Sys. Debian-Ubuntu.pdf"", aut. Tomaszek <d3bkowski@gmail.com>, z d. 2025-12-23, wto.

UWAGA z d. 2022-12-23: Po zainstalowaniu sys. i ustawieniu partycji /tmp i /var z blokadą urucha-

miania prog. okazało się, że niemożna aktualizować ani instalować pakietów.

4.6 Pamięć Wymiany²⁷

Partycja swap lub plik swap realizuje funkcję pamięci wirtualnej. Część dysku pracuje wtedy jako przedłużenie pamięci RAM. Jest to ratunek dla sys. op. gdy prog. zaczynają zajmować całą pamięć operacyjną.

Gdy zdarza się, że sys. bardzo zamula to znak, że włącza się swap. W takiej sytuacji należy dokupić fizyczne rozszerzenie pamięci RAM.

Innym rozwiązaniem sytuacji gdy kończy się pamięć RAM jest zamykanie najbardziej pamięćozernych procesów.

W sys. op. Linuks pamięć wymiany może mieć postać partycji swap lub pliku swap.

Partycja swap działa szybciej niż plik swap. Jest tak dla tego, że używając partycji swap nie ma potrzeby dostępu do dysku za pośrednictwem f. sys. plików.

Partycja swap może szybko zabić dysk SSD, NVM i partyk USB. Jest tak gdyż są one pamięcią typu Flasz której cechą jest to, że ma ograniczoną liczbę zapisów i odczytów.

Współczesne komp. powinny mieć tyle pamięci RAM by nie było konieczności włączania pamięci wymiany.

4.7 Generowanie Silnego Hasła

Generalnie mamy 4 rodzaje haseł. Wymieńmy je wg stopnia komplikacji:

1. Wyłącznie z małych lub wyłącznie z wielkich liter;
2. Wyłącznie z małych lub wielkich liter;
3. Wyłącznie z liter lub cyfr;
4. Z dowolnych znaków drukowanych.

Hasła o długości do 6 znaków są łatwe do złamania. Dlatego żadne piny nie są dłuższe (ma to znaczenie dla służb i dla tajnej policji).

²⁶ W j. ang.: journaling

²⁷ W j. ang.: swap

Są w sys. op. Linuks prog. do generowania haseł: **makepasswd**, **pwgen** oraz **bardziej zaawansowany apg**.

Instalują je polecenia:

```
sudo apt install makepasswd
sudo apt install pwgen
sudo apt install apg
```

Wśród tych prog. apg wyróżnia się tym, że domyślnie generuje hasła podobne do angielskich słów. Przez co niektórym może być łatwiej je zapamiętać.

```
apg -m 12 -x 12
octyanyitDa
RyclacpesI15
GimpitBogLux
lurAgzizamhy
VewedjitCet4
sasGentOicks
```

Jednak wydaje się, że opcja -a 1 generuje dużo silniejsze hasła, bo używa bardziej różnorodnych kombinacji znaków.

```
apg -m 12 -x 12 -a 1
n9>H*nM1h}o0
Z.0m\#f<|JSJ
lWw*r}_Y9Ir5
w%:-PgrR=0Qs
ng,uD{00jb<N
LXpzqE+=!>$_
```

Oczywiście tych generatorów haseł możesz używać do generowania silnych haseł do wszystkich możliwych celów (szczególnie w sieci Internet).

4.7.1 cracklib-check

Mogło się zdarzyć, że nie skorzystałeś z generatora haseł tylko sam je sobie wymyśliłeś. W takim przypadku warto spr. jak hasło jest silne.

```
sudo apt install cracklib-runtime
```

Zanim wywołasz polecenie sprawdzające twoje hasło zwróć uwagę by je rozpocząć spacją (poniżej jest ona zaznaczona na czerwono).

Polecenie poprzedzone spacją nie zostanie dodane do historii poleceń powłoki²⁸.

²⁸ Historia wydawanych poleceń znajduje się w pliku: **\$HOME/.bash_history** .

Teraz sprawdź swoje hasło poleceniem:

```
echo "TWOJE HASŁO" |
/usr/sbin/cracklib-check
```

Możesz w ten sposób sprawdzać wszelkie inne używane przez Ciebie hasła (np. hasła do banków czy do sklepów Internet).

W razie gdybyś zapomniał poprzedzić pow. polecenie spacją: w konsoli, jeśli naciśniesz strzałkę w górę i zobaczysz polecenia spr. twoje hasła oznacza to, że zostały dodane do historii. W takim przypadku powinieneś wyczyścić historię konsoli wydając poniższe polecenia:

```
history -c
rm ~/.bash_history
```

4.7.2 John The Ripper

Po instalacji i konfiguracji sys. op. Linuks możesz od czasu do czasu sprawdzić siłę haseł użytkowników w sys. prog. John the Ripper. Ten łączacz haseł działa na plikach z sumami obliczonymi z haseł (w przeciwieństwie do cracklib-check który działał bezpośrednio na hasłach).

Oto polecenia instalujące tego łączacza haseł wraz ze słownikiem polskim:

```
sudo apt install john -y
sudo apt install wpolish
```

Aby sprawdzić siłę haseł w sys. należy skopiować plik z hasłami do katalogu tmp:

```
sudo /usr/sbin/unshadow /etc/passwd
/etc/shadow > /tmp/crack.password.db
```

A następnie uruchomić łączacza:

```
john /tmp/crack.password.db
```

Przy dobrych hasłach ten prog. nie powinien sam się zakończyć (powinien bez końca analizować silne hasła).

Po tej operacji należy usunąć plik tymczasowy:

```
sudo rm -f /tmp/crack.password.db
```

Tej ostatniej operacji nie można zapomnieć, gdyż potencjalnie /tmp/crack.password.db może być luką bezpieczeństwa.

Prog. John the Ripper to taka ciekawostka historyczna, bo ten prog. nie wykorzystuje proc. wielordzeniowych, czyli działa w jednym wątku, co jest kompletnym anachronizmem.

4.7.3 Zmiana Hasła

Jeśli kiedyś będziesz chciał zmienić swoje hasło w sys. użyj polecenia

```
passwd
```

Wtedy podaj stare hasło i 2x nowe.

passwd nie pozostawia haseł w historii poleceń powłoki.

5 Instalacja Sys. Op. Linuks

5.1 W Czasie Instalacji Sys. Op. Nie Łącz Się z Siecią Lokalną Ani z Siecią Internet

Nawet gdy do tego zachęcają. Podczas instalacji sys. jest bezbronny.

5.2 Wybierz Punkty Montowania Przygotowanych Partycji

Wybierz ręczny podział na partycje.

A tam ustaw katalogi montowania dla każdej z nich. Zrób to zgodnie z podziałem dysku na partycje jaki wprowadziłeś w ramach przygotowań do instalacji.

5.3 Wprowadź Hasło Jakiego Wygenerowałeś

6 Konf. Stacji Roboczej Linuks Po Instalacji

6.1 Skonfiguruj sudo

6.1.1 Dodaj Siebie Do Grupy sudo

Jest to konieczne byś mógł normalnie wykonywać czynności administracyjne w sys. op. Linuks bez używania konta root ani polecenia su. Robisz to poleceniem:

```
sudo gpasswd -a $USER sudo
```

Wynik możesz sprawdzić poleceniem:

```
id $USER
```

6.1.2 Ustaw sudo Tylko Dla Siebie

Dbaj o to by żaden inny użytkownik w twoim sys. nie należał do grupy sudo. Aby to spr. należy użyć polecenia:

```
getent group sudo
```

Powinno dać w wyniku tylko Ciebie.

Aby usunąć użytkownika z grupy sudo należy użyć polecenia:

```
sudo gpasswd -d USER sudo
```

6.1.3 Włącz Sobie Użycie sudo Bez Hasła

Zrób kopię pliku /etc/sudoers:

```
sudo cp /etc/sudoers /etc/sudoers.org  
sudo nano /etc/sudoers
```

Dodaj linię:

```
$USER ALL=(ALL) NOPASSWD:ALL
```

Tylko zamiast \$USER podaj swój login.

6.2 Skonfiguruj Zaporę Sieciową UFW

Niektóre prog. podają na s. podręcznika man z jakich serwerów korzystają. Taj robi np. whois.

Ruch sieciowy mogą obserwować dzięki prog. netstat, tcpdump i Wireshark.

By się dowiedzieć gdzie prog. usiłuje się łączyć, można użyć strace²⁹.

6.2.1 Domyślne Blokowanie Ruchu Sieciowego Przychodzącego

Ja na swoich komp. konfiguruję UFW tak:

Instaluję, resetuję i włączam zaporę sieciową UFW:

```
sudo apt install ufw
sudo ufw reset
sudo ufw enable
```

Konfiguruję ufw tak by domyślnie blokował cały ruch wchodzący i wychodzący:

```
sudo ufw default deny incoming
```

6.3 Konfiguracja Prog. Gł. Sys. Op. Linuks

Aby dostroić sam prog. gł. sys. op. Linuks należy wyedytować plik:

```
sudo nano /etc/sysctl.d/20-energo-prog-gl.conf
```

I uzupełnij go taką treścią:

```
# Losowe przydzielanie adresów pamięci (mmap, sterta i stos):
kernel.randomize_va_space= 2
# Ponowne uruchomienie po 10s po zawieszeniu jądra:
```

²⁹ Pamiętaj o opcji -f która zapewnia śledzenie również procesów potomnych.

```
kernel.panic= 10
# Włączenie IP spoofing protection:
net.ipv4.conf.all.rp_filter= 1
# Zablokowanie IP source routing:
net.ipv4.conf.all.accept_source_route= 0
net.ipv6.conf.all.accept_source_route= 0
# Ignorowanie rozgłoszeń broadcasts:
net.ipv4.icmp_echo_ignore_broadcasts= 1
# Logowanie fałszowanych pakietów:
net.ipv4.conf.all.log_martians= 1
# Wyłączanie przekazywania pakietów:
net.ipv4.ip_forward= 0
# Brak komunikatów o podejrzanych błędach ICMP:
net.ipv4.icmp_ignore_bogus_error_responds= 1
```

Następnie wydaj polecenie:

```
sudo /lib/systemd/systemd-sysctl
```

Aby spr. aktualne ustawienia związane z rdzeniem sys. op. Linuks użyj polecenia:

```
sudo sysctl --system
```

6.4 Skonfiguruj Partycje

W przypadku gdy się zdecydujemy na proponowany powyżej podział na partycje można ograniczyć możliwości intruza. Ja tak konfiguruję partycje:

```
sudo nano /etc/fstab
```

1. Wyłączam czasy i montowanie przez użytkownika na partycji /:

```
UUID=XXX...XXX /
ext2
defaults,noatime,nodiratime,noiv
ersion,norelatime,nostrictatime,
lazytime,nouser 0 1
```

2. Wyłączam lepki bit, tworzenie urządzeń, czasy i montowanie przez użytkownika na partycjach: /home, /boot, /usr/local, /opt, /tmp i /var:

```
UUID=XXX...XXX /home ext4
defaults,nosuid,nodev,noatime,no
diratime,noiversion,norelatime,n
ostrictatime,lazytime,nouser 0 2
```

3. Wyłączam uruchamianie, lepki bit, tworzenie urządzeń, czasy i montowanie przez użytkownika w pamięci współdzielonej:

```
none /run/shm
tmpfs
rw,noexec,nosuid,nodev,noatime,nodiratime,noiversion,norelatime,
nostrictatime,lazytime,nouser 0
0
```

6.5 Wyłącz Plik Wymiany

Jak podałem wyżej plik wymiany może zabić dysk SSD, dlatego w razie gdyby komp. zamulał należy dokupić pam. RAM, a swap należy wyłączyć.

Na czas bieżącej sesji swap można wyłączyć poleceniem:

```
sudo swapoff -a
```

Natomiast na trwale wyłącza się go edytując plik:

```
sudo nano /etc/fstab
```

Tam trzeba zakomentować (znakiem #) linię:

```
# /swapfile    none    0          swap
sw            0      0
```

Na Ubuntu Serwer jest to:

```
# /swap.img    none    swap    sw
0             0
```

Ta zmiana zostanie uwzględniona po ponownym uruchomieniu sys.

Potem usuń pliki wymiany. Na stacji roboczej:

```
sudo rm /swapfile
```

Na Ubuntu Serwer:

```
sudo rm /swap.img
```

6.6 Włącz Automatyczne Ubijanie Zbyt Żarłocznego Procesu

Nie wiem też nic na temat ustawienia które przy wyczerpywaniu pamięci ubija najbardziej żarłoczny proces.

Powłoka Bash może działać w kilku trybach: logowania, wsadowym i interaktywnym.

W przypadku trybu logowania: cytat:

"[...] w pierwszej kolejności czyta i wykonuje polecenia z pliku /etc/profile, jeśli takowy istnieje. Po odczytaniu tego pliku, szuka ~/.bash_profile, ~/.bash_login i ~/.profile, w tej kolejności [...]"

, źródło: man bash, aut. anonim, wer. z d. 2016-08-26, pią.

Czyli te skrypty są uruchamiane raz po zalogowaniu użytkownika.

W przypadku trybu wsadowego: cytat:

"[...] szuka w środowisku zmiennej BASH_ENV, interpretuje jej wartość, jeśli ją znalazł, i używa otrzymanej wartości jako nazwy pliku do odczytania i wykonania."

, źródło: man bash, aut. anonim, wer. z d. 2016-08-26, pią.

W przypadku trybu interaktywnego: cytat:

"[...] bash czyta i wykonuje polecenia z /etc/bash.bashrc i ~/.bashrc, jeśli takie pliki istnieją"

, źródło: man bash, aut. anonim, wer. z d. 2016-08-26, pią.

Te tryby i uruchamiane skrypty mają takie praktyczne znaczenie, że umożliwiają konf. powłoki globalnie dla wszystkich użytkowników z rozróżnieniem trzech powyższych trybów. Umożliwia to ustawienie np. limitów pamięciowych dla wszystkich użytkowników w pliku /etc/profile. Dodatkowo rozróżnia się limity "miękkie" i "twarde". Twarde są nieprzekraczalne a miękkie są standardowo ustawiane. Limity miękkie można zmieniać w \$HOME/.profile.

Polecenie ulimit pozwala na określenie różnych limitów dla uruchamianych prog. Aby ustawić limit pamięci wirtualnej w prog. należy wyedytować plik:

```
nano /etc/profile      # Dla wszystkich
użytkowników.
```

lub

```
nano $HOME/.profile  # Dla konkretnego
użytkownika.
```

Należy dodać takie linie:

```
ulimit -m $((18*1024*1024))
```

³⁰To jest limit rzeczywistego użycia pamięci przez proces użytkownika.

```
ulimit -v $((118*1024*1024))
```

Moim zdaniem ta wart. to nie jest wielkość pam. wirt. (w sensie swap) tylko całkowita ilość zaalokowanej pamięci przez proces użytkownika (czyli tyle pamięci proces zażądał od sys. operacyjnego).

Jak jakiś prog. nagle zostanie zamknięty, to znaczy, że ulimit -v lub ulimit -m jest za mały. Oznacza to, że właśnie miałeś próbę włamania typu "przepełnienie bufora"³¹.

Warto też dodać limit na ilość uruchamianych przez użytkownika procesów (licząc wątki - jeden prog. może uruchamiać wiele wątków):

```
ulimit -u 1018
```

30 Ta dziwna konstrukcja z $\$(())$ to wyrażenie matematyczne w Bashu obliczające ile KB jest w 18GB oraz niżej w 118GB.

31 Akregator (czytnik RSS) potrafi wykorkować przy niskich wart. limitów pam., podobnie prog. Java (bez 6GB nawet nie odpalą), Google Chrome zajmuje 1TB pam. wirt. tak więc wymusza wyłączenie ulimit, Firefox zachowuje się b. podobnie, obecnie (2023r.) rozw. jest użycie przeglądarki Falcon (co ciekawe na silniku Chrome).

6.7 Zaostrz Prawa Dostępu Do Katalogów Użytkowników

6.7.1 Katalogi Domowe

Prawa dostępu do kat. domowych użytkowników są domyślnie zbyt słabe bo pozwalają każdemu zalogowanemu w sys. na przeglądanie i kopiowanie moich prywatnych danych.

Wyłączam grupom i pozostałym użytkownikom dostęp do kat. domowych użytkowników i root:

```
sudo chmod -R go-rwx /home/* /root
```

Gdybym chciał wyłączyć grupom i innym użytkownikom dostęp do mojego kat. domowego wydałbym polecenie:

```
chmod -R go-rwx $HOME
```

Przypisuję dla siebie wszystkie pliki i katalogi w moim katalogu:

```
chown -R $USER:$USER $HOME
```

Tego polecenia należy użyć dla każdego użytkownika na naszym komp.

W tym celu najpierw zaloguj się na konsolę każdego z nich poleceniem:

```
su - USER
```

Gdzie USER to login użytkownika.

Po tych poleceniach udostępnianie plików bezpośrednio z katalogów domowych nie będzie działać. Bo to wymaga dostępu użytkowników z grup do jakich należę (np. samba, ftp czy www).

Po tych poleceniach nadal normalnie będzie działać przeglądarka, klient pocztowy.

6.7.2 UMASK

Maska UMASK definiuje, dla każdego użytkownika osobno, jakich uprawnień **NIE** mają mieć nowe pliki i katalogi.

Dla przypomnienia:

"drwxrwxrwx

to flagi dostępu, które można ustawić dla kat. i plików. Jeśli wszystkie flagi rwx są ustawione tworzą one liczby, np.:

rwx	111	7	odczyt, zapis, uruchomienie
rw	110	6	odczyt, zapis
r	100	4	tylko odczyt
w	010	2	tylko zapis
x	001	1	tylko uruchomienie

Ustawiona flaga d oznacza, że to kat. w przeciwnym wypadku może to być plik, link symboliczny lub urządzenie."

Czyli gdy UMASK ma ona wartość 077 to, dla nowych kat. i plików, ani grupa ani pozostali użytkownicy nie będą mieli prawa odczytu, zapisu ani wykonania.

Natomiast Ty będziesz miał te (pełne) prawa, czyli 600 dla nowych plików i 700 dla nowych katalogów.

6.7.2.1 UMASK Globalny

W pliku

```
sudo nano /etc/login.defs
```

ustaw:

```
UMASK 077  
USERGROUPS_ENAB no
```

Ta druga opcja, jeśli jest włączona, powoduje że efektywnie UMASK ma wartość 007, a nie o to chodzi...

6.7.2.2 Problemy z Globalnym UMASK

Po globalnym zaostrzeniu flagi UMASK pojawią się problemy z menadżerami pakietów APT i pip (Python 2 i 3) i pewnie z innymi.

Rozwiązania znam 3:

1. Konfigurować umask lokalnie dla każdego użytkownika zamiast globalnie.
2. W przypadku pip można instalować skrypty Pythona bez sudo, czyli lokalnie, w katalogu użytkownika, czyli tylko dla siebie;

3. W przypadku pip można instalować skrypty globalnie w sys., dla wszystkich użytkowników poleceniem `sudo pip3 XXX`. Następnie wywołać takie polecenie:

```
sudo chmod -R go+rx  
/usr/local/lib/python3.8
```

6.7.2.3 UMASK Lokalny

Warto rozważyć ustawianie umask tylko sobie i zwykłym użytkownikom, a root-a zostawić w spokoju. W tym celu w pliku:

```
nano $HOME/.profile
```

Należy dodać linię:

```
umask 077
```

6.7.3 DIR_MODE

DIR_MODE określa domyślne prawa dostępu do nowo tworzonego kat. użytkownika (podkatalogi z nazwami użytkowników w kat /home). Domyślnie jest to 0755 czyli wszyscy mają możliwość odczytu łącznie z atrybutami plików. Aby ten nonsens zmienić edytując:

```
sudo nano /etc/adduser.conf
```

ustawiam:

```
DIR_MODE=0700
```

Czyli zapewniam wyłącznie sobie odczyt, zapis i wykonanie.

6.8 Wyłącz Konsolę Dla Nowych Użytkowników

W pliku:

```
sudo nano /etc/default/useradd
```

zmień SHELL na:

```
SHELL=/usr/sbin/nologin
```

W pliku

```
sudo nano /etc/adduser.conf
```

zmień DSHELL na:

```
DSHELL=/usr/sbin/nologin
```

6.9 firejail

Koncepcja ograniczania prog. komp. tak by nie mogły kraść i wysyłać moich prywatnych danych w świat jest bardzo dobra. Te prog. nazywane są piaskownicami. Prog. te bazują na plikach profili które szczegółowo definiują do czego prog. ma dostęp, a do czego dostępu nie ma. Do tych prog. zaliczamy firejail (w j. ang. Friejail). Jest on przykrywką dla AppArmor (w Debian/Ubuntu) i SeLinux (w RedHat).

Przykładowo gdy uruchomimy Thunderbird w firejail, to Thunderbird będzie miał dostęp tylko do kat. \$HOME/Pobrane i paru plików konf. w \$HOME. Tak więc nic nie jest w stanie nam ukraść.

Sposób użycia prog. konsolowego strace w celu wykrywania zasobów koniecznych do działania prog. jest opisany w art. [idealna-recenzja-linux-mag-pl-2024-05].

Niestety obecnie firejail nie pozwala na konf. zapory sieciowej dla każdego prog. z osobna.

6.9.1 Instalacja firejail

```
sudo apt install firejail
```

6.9.2 Włączenie firejail

Włączenie firejail jest dwu etapowe:

1. Najpierw trzeba utworzyć w kat. /usr/local/bin linki symboliczne o nazwach kontrolowanych prog. Wszystkie one kierują do prog. /usr/bin/firejail . Przy uruchomieniu spr. on jaki link do niego prowadził i uruchamia w piaskownicy prog. o tej nazwie, tylko z kat /usr/bin . Działa to prawidłowo, bo prog. uruchamiany w skróconej formie jest wyszukiwany najpierw w /usr/local/bin a jak tam go nie ma to szukany jest w /usr/bin . Linki symb. w /usr/local/bin tworzy polecenie:

```
sudo firecfg
```

2. Następnie w kat. domowym każdego użytkownika trzeba usunąć ścieżki /usr/bin/ ze wszyst-

kich poleceń w plikach *.desktop³² by uruchamiały one prog. z /usr/local/bin (bo ma on wyższy priorytet niż /usr/bin – jw.). Robi to polecenie (bez sudo, jednak trzeba go użyć dla każdego użytkownika w systemie):

```
firecfg --fix
```

6.9.3 Uruchamianie Prog. w Piaskownicy firejail i Bez Niej

Po tych zabiegach uruchamianie prog. odbywa się wg schematu:

```
/usr/bin/thunderbird # Uruchomi się bez piaskownicy.  
thunderbird # Uruchomi się w piaskownicy.
```

Czyli podając pełną ścieżkę (tu: /usr/bin/XXXXX) pomija się firejail. Natomiast wydając skrócone polecenie prog. uruchamiany jest w piaskownicy.

6.9.4 Spr. Czy Prog. Jest Uruchomiony w Piaskownicy firejail

```
firejail --list
```

6.9.5 Strojenie firejail

Uprawnienia prog. zdefiniowane w kat. /etc/firejail są bardzo restrykcyjne, a czasem wręcz niezyciowe. Dla niektórych prog. w ogóle brak profili firejail.

To że profile firejail nie odpowiadają w 100% naszym potrzebom nie znaczy, że firejail jest zły. Oznacza to, że firejail trzeba dostrajać zamiast się niepotrzebnie denerwować.

Formaty plików /etc/firejail/*.profile oraz \$HOME/.config/firejail/*.local są takie same. Ich opis jest na nietypowej s. podręcznika systemowego:

```
man firejail-profile
```

³² Są to pliki opisujące skróty z ikonami na pulpicie i w menu Start.

Mogę dodać, że obecnie prawie wszystkie nieuprzywilejowane prog. jakich na co dzień używam uruchamiam w firejail.

Tu podam kilka przykładów jak dostrajam firejail. Omówię profile przykładowych prog.: przeglądarki i klienta pocztowego, IDE, procesora tekstu i prog. graf. i jako bonus konf. odtwarzacza VLC.

1. Przeglądarka Brave (którą zalecam, bo można opłacić usługę wyszukiwarki, przez co unika się "skrytego zadłużania"). Mój profil `HOME/.config/firejail/brave.local` wygląda tak:

```
protocol unix,inet,inet6
```

```
private-dev
```

```
whitelist
```

```
HOME/.config/BraveSoftware  
whitelist HOME/.cache/BraveSoftware
```

```
noblacklist HOME/+Ściągnięte  
whitelist HOME/+Ściągnięte  
noexec HOME/+Ściągnięte
```

```
blacklist HOME/.bash_history  
blacklist HOME/.config/chromium  
blacklist HOME/.gnupg  
blacklist HOME/.lessht  
blacklist HOME/.mozilla  
blacklist HOME/.ssh  
blacklist HOME/.zsh_history
```

Chodzi w nim o to, że ma dostęp do d-bus, protokołów internetowych, lokalnych gniazd UNIX, ma dostęp do "wirtualnego" kat. /dev jedynie z kilkoma podstawowymi urządzeniami, ma dostęp do kat. z konf. i do kat. `HOME`/+Ściągnięte, jednak niczego z niego nie może uruchamiać.

2. Klient pocztowy Thunderbird (można za niego wpłacać darowizny). Mój profil `HOME/.config/firejail/thunderbird.local` wygląda tak:

```
protocol unix,inet,inet6
```

```
nodbus
```

```
private-dev
```

```
whitelist HOME/.thunderbird
```

```
noblacklist HOME/+Ściągnięte  
whitelist HOME/+Ściągnięte
```

```
noexec HOME/+Ściągnięte
```

```
blacklist HOME/.bash_history  
blacklist HOME/.config/chromium  
blacklist HOME/.gnupg  
blacklist HOME/.lessht  
blacklist HOME/.ssh  
blacklist HOME/.zsh_history
```

Chodzi w nim o to, że nie ma dostępu do d-bus, ma dostęp do protokołów internetowych, lokalnych gniazd UNIX, "wirtualnego" kat. /dev jedynie z kilkoma podstawowymi urządzeniami, ma dostęp do kat. ustawień i do kat. `HOME`/+Ściągnięte, jednak niczego z niego nie może uruchamiać.

3. Qt Creator – IDE dla programistów kodujących w j. C++. W `HOME/.config/firejail/qtcreator.local` mam taki wpis:

```
net none  
private-tmp  
ignore seccomp
```

```
whitelist HOME/.config/QtProject  
whitelist HOME/.cache/QtProject  
whitelist HOME/.config/kdeglobals
```

```
whitelist HOME/+Energokod  
whitelist HOME/+Ściągnięte  
whitelist HOME/x-instal  
whitelist HOME/zrodla
```

```
blacklist HOME/.ssh  
blacklist HOME/.gnupg
```

```
blacklist /opt
```

W tym profilu chodzi o to, że: nie ma dostępu do protokołów internetowych (czyli nie ma dostępu do sieci Internet), ma dostęp do "wirtualnego" kat. /dev jedynie z kilkoma urządzeniami, ma dostęp do ustawień własnych i do ustawień pulpitu, ma dostęp do kat. z proj.

4. Libreoffice - pakiet biurowy. Mój `HOME/.config/firejail/libreoffice.local` wygląda tak:

```
net none  
nodbus  
private-tmp
```

```
whitelist HOME/.config/libreoffice
```

```
whitelist HOME/.config/kdeglobals  
read-only HOME/.config/kdeglobals
```

```
whitelist HOME/+Dokumenty
```

```
noexec ${HOME}/+Dokumenty
```

```
noblacklist ${HOME}/+Dokumenty  
whitelist ${HOME}/+Dokumenty  
noexec ${HOME}/+Dokumenty
```

```
noblacklist ${HOME}/+Obrazy  
whitelist ${HOME}/+Obrazy  
noexec ${HOME}/+Obrazy
```

```
noblacklist ${HOME}/+Ściągnięte  
whitelist ${HOME}/+Ściągnięte  
noexec ${HOME}/+Ściągnięte
```

```
noblacklist ${HOME}/+Szablony  
whitelist ${HOME}/+Szablony  
noexec ${HOME}/+Szablony
```

```
blacklist /opt
```

W tym profilu chodzi o to, że: nie ma dostępu do protokołów internetowych (czyli nie ma dostępu do sieci Internet), nie ma dostępu do d-bus, ma dostęp do "wirtualnego" kat. /tmp, ma dostęp do ustawień własnych i do ustawień pulpitu, ma dostęp do kat. \$HOME/+Dokumenty, \$HOME/+Szablony, \$HOME/+Ściągnięte i \$HOME/+Obrazy .

5. Gimp - edytor obrazów. Mój profil \$HOME/.config/firejail/gimp.local, wygląda tak:

```
net none  
nodbus
```

```
private-tmp
```

```
whitelist ${HOME}/.config/GIMP  
whitelist ${HOME}/.local/share/GIMP
```

```
whitelist ${HOME}/.config/kdeglobals  
read-only ${HOME}/.config/kdeglobals  
whitelist ${HOME}/.config/gtk-3.0  
read-only ${HOME}/.config/gtk-3.0  
whitelist ${HOME}/.local/share/icons  
read-only ${HOME}/.local/share/icons
```

```
noblacklist ${HOME}/+Dokumenty/Loga  
whitelist ${HOME}/+Dokumenty/Loga  
noexec ${HOME}/+Dokumenty/Loga
```

```
noblacklist ${HOME}/+Obrazy  
whitelist ${HOME}/+Obrazy  
noexec ${HOME}/+Obrazy
```

```
noblacklist ${HOME}/+Ściągnięte  
whitelist ${HOME}/+Ściągnięte  
noexec ${HOME}/+Ściągnięte
```

```
blacklist /opt
```

W tym profilu chodzi o to, że: nie ma dostępu do protokołów internetowych (czyli nie ma dostępu do sieci Internet), nie ma dostępu do d-bus, ma dostęp do "wirtualnego" kat. /tmp, ma dostęp do ustawień własnych i do ustawień pulpitu, ma dostęp do kat. \$HOME/+Dokumenty/Loga, \$HOME/+Obrazy i \$HOME/+Ściągnięte .

6. VLC - odtwarzacz filmów i muzyki - mój profil \$HOME/.config/firejail/vlc.local wygląda tak:

```
net none
```

```
private-tmp  
private-cache
```

```
whitelist ${HOME}/.config/vlc
```

```
whitelist ${HOME}/.config/kdeglobals  
read-only ${HOME}/.config/kdeglobals
```

```
whitelist ${HOME}/+Muza  
read-only ${HOME}/+Muza  
noexec ${HOME}/+Muza
```

```
whitelist ${HOME}/+Filmy  
read-only ${HOME}/+Filmy  
noexec ${HOME}/+Filmy
```

```
whitelist ${HOME}/+Ściągnięte  
read-only ${HOME}/+Ściągnięte  
noexec ${HOME}/+Ściągnięte
```

```
blacklist /opt
```

W tym profilu chodzi o to, że: nie ma dostępu do protokołów internetowych (czyli nie ma dostępu do sieci Internet), ma dostęp do d-bus (aby działały klawisze multimedialne na klaw.), ma dostęp do "wirtualnego" kat. /tmp i cache, ma dostęp do ustawień własnych i do ustawień pulpitu, ma dostęp do kat. \$HOME/+Muza, \$HOME/+Filmy i \$HOME/+Ściągnięte .

6.9.6 Dodawanie Brakujących Profili firejail

6.9.6.1 Aut. Tworzenie Nowego Profilu firejail

Ten roz. napisałem wg. wskazówek ChatGPT (OpenAI, model GPT-5.5) po odp. na pyt.: "firejail --build=krita.profile \ --appimage ~/AppImages/krita-5.2.9-

x86_64.AppImage Tego nie znałem! Objaśnij mi to bliżej." z d. 2026-06-17, śro.

Na pocz. samo śledzenie:

```
firejail --trace vlc
```

, lub dla paczek AppImage:

```
firejail --trace --appimage  
~/AppImages/krita.AppImage
```

Potem typowa praca parę min., a nast. aut. generowanie profilu:

```
firejail --build=vlc.profile vlc
```

, lub dla paczek AppImage:

```
firejail --build=krita.profile  
--appimage ~/AppImages/krita.AppImage
```

I znowu praca parę min. A potem zamknięcie prog. i ręczne dopracowanie nowego profilu firejail.

6.9.6.2 Ręczne Tworzenie Nowego Profilu firejail

[Powtórzenie z roz. Strojenie firejail]

Formaty plików /etc/firejail/*.profile oraz \$HOME/.config/firejail/*.local są takie same. Ich opis jest na nietypowej s. podręcznika systemowego:

```
man firejail-profile
```

[koniec powtórzenia.]

Procedura dodawania pliku *.profile dla nowego prog. (nazwijmy go "nazwa_programu") jest taka:

1. Tworzenie pliku profile:

Plik ten musi mieć nazwę: nazwa_progarmu.profile.

2. Kopiowanie pliku profile:

Plik nazwa_progarmu.profile musi trafić do katalogu:

```
/etc/firejail
```

3. Dodawanie nazwa_progarmu do listy prog. kontrolowanych przez firejail:

Należy, zrobić kopię zapasową:

```
sudo cp  
/usr/lib/x86_64-linux-gnu/firejail/fire  
ecfg.config /usr/lib/x86_64-linux-  
gnu/firejail/firecfg.config.org
```

Następnie na jego koniec dodać nazwa_progarmu i cały plik firecfg.config przepuścić przez polecenie:

```
cat  
/usr/lib/x86_64-linux-gnu/firejail/fir  
ecfg.config | sort | uniq | sudo  
tail  
/usr/lib/x86_64-linux-gnu/firejail/fir  
ecfg.config.sort
```

Na koniec należy zmienić nazwę na org.:

```
sudo mv  
/usr/lib/x86_64-linux-gnu/firejail/fir  
ecfg.config.sort /usr/lib/x86_64-  
linux-gnu/firejail/firecfg.config
```

4. Ponowna konfiguracja firejail:

```
sudo firecfg --clean  
sudo firecfg  
firecfg --fix
```

Taka uwaga praktyczna związana z tworzeniem własnych profili dla piaskownicy firejail: ja zwykle tworzę brakujący profil z jedną linią, np.: w pliku /etc/firejail/assistant.profile mam tylko:

```
include assistant.local
```

Natomiast całą konf. tego profilu mam w \$HOME/.config/firejail/assistant.local :

```
net none  
nodbus
```

```
private-tmp  
private-cache
```

```
nosound
```

```
whitelist ${HOME}/.config/kdeglobals  
read-only ${HOME}/.config/kdeglobals
```

```
whitelist ${HOME}/.config/fontconfig  
whitelist ${HOME}/.cache/fontconfig
```

```
whitelist ${HOME}/.local/share/icons  
whitelist ${HOME}/.local/share/color-  
schemes
```

```
blacklist /opt
```

To powoduje, że wszystkie moje profile Ognistego Wiedzenia trzymam w jednym miejscu, czyli w kat.

```
$HOME/.config/firejail
```

6.9.7 Paczki AppImage

Założmy, że trzymasz AppImage w ~/AppImages/.

```
nano ~/bin/krita:
```

wklej:

```
#!/bin/sh
firejail --appimage --profile=krita
~/AppImages/krita-5.2.9-
x86_64.AppImage
```

i:

```
chmod +x ~/bin/krita
```

Od tej chwili:

```
krita
```

uruchamia AppImage w Firejail.

6.9.8 Globalne Wyłączenie firejail

Normalnie nie jest potrzebne wyłączenie firejail.

[Powtórzenie z roz. Uruchamianie Prog. w Piaskownicy firejail i Bez Niej]

```
/usr/bin/thunderbird # Thunderbird
uruchomi się bez piaskownicy
thunderbird # Thunderbird
uruchomi się w piaskownicy
```

[Koniec powtórzenia.]

Jednak gdy chcesz koniecznie wyłączyć firejail, to znam dwie metody:

```
sudo firecfg --clean
reboot
```

albo:

```
sudo apt remove --purge firejail
reboot
```

6.10 Skonfiguruj Sieć

Do konf. sieci w sys. Ubuntu używam netplan. W netplan każdą kartę sieciową kontroluje się przez pliki yaml, które umieszcza się w kat. /etc/netplan.

Pamiętaj \$TWOJE_IP to adres twojego kompa w sieci lokalnej jaki teraz sobie wymyślisz i jaki będzie zwracać polecenie ip a gdy już pomyślnie skonfigurujesz sieć i do niej się połączysz.

Zalecam konfigurację statycznego IP. Ma to plus taki, że jak pamiętasz swoje IP, to łatwo stwierdzić, czy inne kompy widzą twój sys. op. Linuks, czy nie (prog. ping). Drugą sprawą jest to, że można sobie zapewnić lepszą symbolikę niż przy DHCP.

Aby skonfigurować sieć musisz podjąć parę decyzji:

1. Jak chcesz skonfigurować sieć w twoim sys. op. Linuks?

Odradzam konfigurację sieci z poziomu pulpitu, bo:

- 1.1 Nie zadziała dla wszystkich użytkowników;
- 1.2 Nie zadziała też w sytuacji awaryjnej, gdy nie ma możliwości uruchomienia pulpitu.

2. Jaki ma być adres twojej sieci prywatnej?

Do wyboru masz parę sieci wymieniłem je w roz. Budowa Sieci Internet.

3. Jakich typów masz karty sieciowe?

Konfiguracja się różni w przypadku kart kablowych i radiowych.

4. Jak się nazywają twoje karty sieciowe w sys. op. Linuks?

```
sudo lshw -C network
[...]
logical name: XXXXXXXX
[...]
```

XXXXXXXX jest nazwą twojej karty sieciowej w sys. op. Linuks.

5. Jak nazywają się twoje sieci WiFi?

```
nmcli device wifi list
```

6. Jak skonfigurować karty sieciowe?

Przykładowy plik dla karty sieci kablowej może mieć taką postać:

```
network:
  ethernets:
    eXXXXX:
      addresses:
        - TWOJE_IP/24
      activation-mode: manual
      dhcp4: no
      dhcp6: no
      nameservers:
        addresses: [1.1.1.1,1.0.0.1]
      version: 2
      renderer: NetworkManager
```

eXXXXX to nazwa karty sieciowej. TWOJE_IP/24 oznacza adres IP i sieć. Sieć jest rozpoznawana przez maskę bitową, tu są to 24 bity czyli 3 bajty. Oznacza to, że część adresu dotycząca sieci to 24bity z 32, a adresy komp. w tej sieci to reszta, czyli 8 bitów z 32. Gdy mamy 8 bitów, to znaczy, że mamy do dyspozycji 255 wart. (jednak w IP są zarezerwowane wart. specjalne takie jak 255). Reszta jest chyba jasna.

Przykładowy plik dla karty sieci radiowej może mieć taką postać:

```
network:
  wifis:
    wXXXXXX:
      access-points:
        "TWOJA_SIEĆ_WIFI":
          password: "XXXXXXXXXXXX"
      activation-mode: manual
      dhcp4: yes
      dhcp6: no
      dhcp4-overrides:
        use-dns: no
      nameservers:
        addresses: [1.1.1.1,1.0.0.1]
      version: 2
      renderer: NetworkManager
```

wXXXXXX to nazwa karty sieciowej, "TWOJA_SIEĆ_WIFI" to identyfikator sieci Wi-Fi (TAK! Z tymi podwójnymi apostrofami.). "XXXXXXXXXXXX" to hasło do sieci Wi-Fi (TAK! Z tymi podwójnymi apostrofami.). Reszta jest chyba jasna.

Konfigurację standardowo kończymy poleceniem aktywującym zmiany:

```
sudo netplan apply
/etc/netplan/TWÓJ_PLIK_KONF.yaml
```

TERAZ NALEŻY PODNIEŚĆ POŁĄCZENIE SIECIOWE W CELU UZYSKANIA POŁ. Z INTERNET.

Robi to polecenie:

```
sudo nmcli dev connect "XXXXX"
```

Oczywiście zamiast XXXXX wstawiasz nazwę swojej karty ethernet, lub nazwę swojej karty WiFi.

6.11 Awaryjne Połączenie z Siecią Internet

Może się zdarzyć, że padnie sieć w twoim komp. i nie ma możliwości samodzielnego naprawienia jej, bo np. brakuje pakietów z repo dystrybucji.

Może też się zdarzyć, że aby w ogóle normalnie połączyć się z siecią lokalną musisz skompilować najpierw sterownik do karty sieciowej. Tego nie zrobisz bez instalacji gcc, make i innych pakietów.

Na te awaryjne sytuacje dziś jest już prosta rada: należy podłączyć sprytny tel. z Androidem kablem USB do kompa. Wtedy wystarczy skonfigurować w sprytnym tel. port USB by udostępniał sieć dla kompa i już można doprowadzić sys. do porządku.

W przypadku gdy sys. sam nie skonfiguruje tego połączenia - jest tak np. na Ubuntu Serwer - wtedy można sobie łatwo poradzić tworząc profil netplan:

```
sudo nano /etc/netplan/usb.yaml
```

Wklej:

```
network:
  ethernets:
    usb0:
      activation-mode: manual
      dhcp4: yes
      dhcp6: no
      dhcp4-overrides:
        use-dns: no
      nameservers:
        addresses: [1.1.1.1,1.0.0.1]
      version: 2
      renderer: NetworkManager
```

Niestety na sys. Android 11 nie można na stałe ustawić adresu sieci więc najprościej ustawić DHCP j.w.

Zainstaluj profil poleceniem:

```
sudo netplan apply
/etc/netplan/usb.yaml
```

Aby się poł. użyj polecenia:

```
sudo nmcli dev connect usb0
```

6.12 Instalacja i Konf. Demona CUPS

CUPS to demon drukowania. Udostępnia on zbędną usługę konfiguracji przez stronę WWW. Jest to zbędne bo to samo można robić z poziomu pulpitu i z linii komend. Aby to wyłączyć edytujemy plik:

```
sudo nano /etc/cups/cupsd.conf
```

Szukam linii:

```
WebInterface Yes
```

I zmieniam na:

```
WebInterface Off
```

Następnie zrestartuj cups:

```
sudo systemctl stop cups.service
sudo systemctl start cups.service
```

Poniżej pokażę uniwersalną konf. drukarki z linii komend: Listę drukarek wyświetla polecenie:

```
lpstat -p
```

Szczegółowe Info o opcjach mojej drukarki uzyskuję poleceniem:

```
lpoptions -p NAZWA_DRUKARKI -l
```

Różni producenci używają różnych nazw dla opcji swoich drukarek!

Dobrze jest mieć zdefiniowane drukarki dla każdego drukowanego formatu. Np. ja drukuję na kartkach A4 i A5, dlatego w sys. op. Linuks mam 2 drukarki.

Obecnie drukarki nie wymagają już dedykowanych sterowników - wszystko obsługuje standard przyjęty ok. 2013 r.

Drukarkę A4 dodaję tak:

```
sudo lpadmin -p NAZWA_DRUKARKI-A4 \
-E -v
ipp://192.168.XXX.YYY/ipp/print \
-m everywhere \
-o PageSize=A4 \
-o Duplex=DuplexNoTumble \
-o cupsPrintQuality=High \
-o printer-is-shared=true \
-L "Pokój w Którym Jest Drukarka"
```

Drukarkę A5 dodaję tak:

```
sudo lpadmin -p NAZWA_DRUKARKI-A5 \
-E -v
ipp://192.168.XXX.YYY/ipp/print \
-m everywhere \
-o PageSize=A5 \
-o Duplex=None \
-o cupsPrintQuality=High \
-o printer-is-shared=true \
-L "Pokój w Którym Jest Drukarka"
```

W tych poleceniach -E znaczy że ma być poł. szyfrowane, -v to docelowy URL, -m to model (tu: "everywhere" znaczy sterownik zgodny z protokołem ipp), -o to opcje drukarki, włączona printer-is-shared jest potrzebna do udostępniania drukarki przez Sambę, -L to jej położenie.

Domyślną drukarkę ustawiam tak:

```
sudo lpadmin -d NAZWA_DRUKARKI-A4
```

Drukarkę domyślną wyświetla polecenie:

```
lpstat -d
```

6.13 SSH

6.13.1 Instalacja ssh

Na stacji roboczej instaluję klienta ssh poleceniem:

```
sudo apt install openssh-client
```

6.13.2 Wygeneruj Parę Kluczy

Uwierzytelnianie należy opierać na kluczach szyfrujących (a nie na hasłach). Nowszym algorytmem (tego SSH w Debian 10 nie rozpoznaje):

```
ssh-keygen -t ed25519
```

Lub starszym:

```
ssh-keygen -t rsa -b 4096
```

6.13.3 Załaduj Publiczne Klucze SSH Na Serwer³³

Aby załadować klucz publiczny na serwer trzeba odblokować na chwilę możliwość logowania hasłem. Jest to dziwne bo wiele poradników karze od razu skonfigurować demona sshd tak by nie można było się logować hasłem tylko kluczami cyfrowymi.

Jeśli nie chcesz ryzykować, to można poniższe pliki skopiować ze stacji roboczej na patyk USB i następnie z patyka USB na serwer.

Klucze cyfrowe trafiają do pliku \$HOME/.ssh/authorized_keys na serwerze.

Aby użyć ssh-copy-id do kopiowania kluczy wykonaj następującą procedurę:

1. Na serwerze odblokuj na chwilę możliwość logowania hasłem:

```
sudo nano /etc/ssh/sshd_config
```

Ustaw:

```
PasswordAuthentication yes
```

2. Na serwerze zrestartuj demona sshd:

```
sudo systemctl restart sshd
```

3. Na stacji roboczej w zależności od użytego algorytmu:

```
ssh-copy-id -i  
$HOME/.ssh/id_ed25519.pub  
UŻYTKOWNIK@SERWER
```

lub:

```
ssh-copy-id -i $HOME/.ssh/id_rsa.pub  
UŻYTKOWNIK@SERWER
```

Gdzie UŻYTKOWNIK to login na zdalnym serwerze. Natomiast SERWER to adres IP lub nazwa domenowa serwera.

³³ Oczywiście należy to zrobić później jak już połączysz się z **Internet**. Tu zostawiłem to by opis **SSH** był w jednym miejscu.

4. Na serwerze zablokuj możliwość logowania hasłem:

```
sudo nano /etc/ssh/sshd_config
```

Ustaw:

```
PasswordAuthentication no
```

5. Na serwerze zrestartuj demona sshd:

```
sudo systemctl restart sshd
```

6.14 Postarzanie Prog. Gł. Sys. Op. Linuks

6.14.1 Blokada Aktualizacji Prog. Gł. Sys. Op. Linuks

Mnie osobiście bardzo dziwi i bardzo niepokoi cotygodniowa aktualizacja prog. gł. w dystrybucjach bazujących na Debianie (w tym w Ubuntu).

Nie wnioskuję co tam oni mieszają, tylko po instalacji wydaję polecenie:

```
sudo apt-mark hold linux-*
```

Aby cofnąć to polecenie należy wydać polecenie:

```
sudo apt-mark unhold linux-*
```

6.14.2 Instalacja Najstarszego Prog. Gł. Sys. Op. Linuks w Repo

Listę dostępnych prog. gł. podaje polecenie:

```
apt list | grep -P 'linux-image-\d+.*'
```

Instaluję też najstarszy prog. gł. Linuksa w repo - u mnie to wer. 5.4.0-26:

```
sudo apt install $(apt list | grep  
'linux-[^-]*-5.4.0-26-generic' | cut -  
d '/' -f1 | tr '\n' ' ')
```

Widać, że jest to operacja dla wtajemniczonych, bo jak się poda jedynie pakiet linux-image-5.4.0-26-generic, to zgłosi błąd! Dopiero ręcznie poda się pełną listę zależności, to można zainstalować wybrany rdzeń.

Do powyższego należy dodać:

```
sudo apt install linux-modules-extra-5.4.0-26-generic
```

Bo bez tego X-y nie odpalą.

6.14.3 Uruchom Ponownie Sys. Komp. Wybierając w boot menu Starą Wer. Prog. Gł. Sys. Op. Linux

6.14.4 Usuwanie Zbędnych Prog. Gł.

Np. aby usunąć prog. gł. Linuksa w wer. 5.4.0-96 należy wykonać polecenie:

```
sudo apt remove --purge $(apt list | grep 'linux-[^-]*-5.4.0-96-generic' | cut -d '/' -f1 | tr '\n' ' ')
```

Widać, że jest to operacja dla wtajemniczonych, bo jak się poda jedynie pakiet linux-image-5.4.0-96-generic, to zgłosi błąd! Dopiero ręcznie poda się pełną listę zależności, to można usunąć wybrany rdzeń. Stąd powyższy skrypt.

Zauważyłem, że z jakiegoś powodu nawet po usunięciu rdzenia w kat. /boot zostają niektóre jego pliki. Rozpoznasz je po numerach tych rdzeni jakie usunąłeś. Usuń z kat. /boot te pliki, np. z kerelem w wer. 5.4.0-96 powiązane są takie pliki:

```
sudo rm -f /boot/System.map-5.4.0-96-generic
sudo rm -f /boot/config-5.4.0-96-generic
```

6.15 Konfiguracja Stacji Roboczej Linuks Dla Programisty

6.15.1 Włącz Zrzuty Obrazów Pam. Prog.

Ponieważ czasem interesują mnie powody nagłego, awaryjnego zatrzymania prog. włączam zrzuty pamięci dla prog. W pliku

```
sudo nano /etc/security/limits.conf
```

ustawiam opcję:

```
* - core 4194304 # 4GB w KB
```

To powoduje, że hard³⁴ i soft³⁵ limit dla pliku z zrzutem pamięci wynosi 4GB.

Edytuję plik:

```
sudo nano /etc/sysctl.d/20-energo-zrzut-zaw-prog.conf
```

I dodaję do niego taką zawartość:

```
# Wyłączenie flagi dającej uprawnienia root-a
fs.suid_dumpable=0
# Podanie katalogu i formatu nazwy pliku dla zrzutów pamięci
# %u to użytkownik, %e to nazwa programu, %p to PID (numer procesu), .core to rozszerzenie pliku
kernel.core_pattern=/var/crash/%u-%e-%p.core
```

Następnie wydaję polecenie wprowadzające powyższe zmiany w działającym rdzeniu sys. op. Linuks:

```
sudo /lib/systemd/systemd-sysctl
```

Aby spr. aktualne ustawienia związane z rdzeniem sys. op. Linuks użyj polecenia:

```
sudo sysctl --system
```

6.16 Konfiguracja Komp. z sys. op. Linuks Dla Nie Programisty

6.16.1 Wyłącz zrzuty prog. gł. i pozostałych prog.

Wyedytuj:

```
sudo nano /etc/security/limits.conf
```

I ustaw:

³⁴ Jest to nieprzekraczalny limit w sys..

³⁵ Jest to domyślny limit użytkownika jaki można zwiększać aż do wart. **hard** lub zmniejszać do 0.

* - core 0

6.17 Ważne Pliki Sys. Op. Linuks

```
sudo chmod 0440 /etc/sudoers
sudo chmod 0600 /etc/cups/cupsd.conf
sudo chmod 0600 /etc/sysctl.conf
```

6.18 Zbędni Użytkownicy

Razem z sys. op. Linuks jest instalowana cała masa niepotrzebnych už. i ich grup, jednak nie da się ich trwale usunąć - po każdym usunięciu wracają oni "auto-magicznie". Jak ktoś chce to niech "próbuje szczęścia":

```
sudo deluser games
sudo deluser mail
sudo deluser news
sudo deluser proxy
sudo deluser www-data
sudo deluser backup
sudo deluser list
sudo deluser irc
sudo deluser gnat
sudo deluser gnats
sudo deluser speech-dispatcher
sudo deluser hplip
sudo deluser uucp
sudo deluser man
```

6.19 Zbędne Grupy Użytkowników

Warto sprawdzić do jakich grup się należy:

groups

Dla normalnego użytkownika wcale nie jest potrzebne należenie do sambashare (udostępnianie plików w sieci SMB czyli dla Windows) ani do dip (używanie modemów tel.). Aby wystąpić z tych grup należy użyć polecenia:

```
sudo gpasswd -d $USER GRUPA
```

Zbędnych grup nie da się trwale usunąć z sys. Linux - po każdym usunięciu wracają oni "auto-magicznie". Jak ktoś chce to niech "próbuje szczęścia":

```
sudo delgroup games
sudo delgroup mail
sudo delgroup news
sudo delgroup proxy
sudo delgroup www-data
sudo delgroup backup
sudo delgroup list
sudo delgroup irc
sudo delgroup speech-dispatcher
sudo delgroup hplip
sudo delgroup uucp
sudo delgroup man
sudo delgroup landscape
sudo delgroup pollinate
sudo delgroup saned
sudo delgroup colord
sudo delgroup gnat
```

6.20 Pliki Bez Właściciela

Nie należy ich usuwać bo rozwała to sys. instalacji pakietów (apt i snap), oraz kontenery np. docker.

6.21 Uszkodzone Linki Symboliczne

Nie należy ich usuwać bo rozwała to sys. instalacji pakietów (apt i snap), oraz kontenery np. docker.

7 Konf. Serwera Linuks Po Instalacji

7.1 Skonfiguruj sudo Tak Jak w Roz. 6.1

7.2 Skonfiguruj Zaporę Sieciową Tak Jak w Roz. 6.2

Oczywiście, że dodatkowo w serwerze trzeba otwierać określone porty UDP i TCP na których są udostępniane

konkretne usługi sieciowe. Dodatkowo w celu popr. bezp. należy usługi sieciowe udostępniać jedynie dla kompów z mojej (lub z twojej) sieci lokalnej.

Przykładowo aby otworzyć port UDP nr 137 w sieci lokalnej 192.168.XXX.0/24 należy:

```
sudo ufw allow from 192.168.XXX.0/24
to any port 137 proto udp
```

Przykładowo aby otworzyć port TCP nr 139 w sieci lokalnej 192.168.XXX.0/24 należy:

```
sudo ufw allow from 192.168.XXX.0/24
to any port 139 proto tcp
```

7.3 Instalacja i Konf. Demona sshd

Na serwerze instaluję demona sshd i klienta ssh poleceniem:

```
sudo apt install ssh
```

Na serwerze oprócz demona sshd mam jeszcze klienta gdyż używam go przez gita by zaciągać moje proj.

7.3.1 Konf. demona sshd

Gdy używasz SSHD na serwerze samodzielnie trzeba skonfigurować tego demona. Wynika to oczywiście ze zbyt łagodnych ustawień domyślnych:

```
sudo nano /etc/ssh/sshd_config
```

Należy dodać następujące linie:

```
PermitRootLogin no
PermitEmptyPasswords no

PubkeyAuthentication yes
PasswordAuthentication no
ChallengeResponseAuthentication no

UsePAM yes

IgnoreRhosts yes
HostbasedAuthentication no

AllowTCPForwarding no
AllowAgentForwarding no
PermitTunnel no
X11Forwarding no
```

```
LoginGraceTime 30
MaxAuthTries 3
```

```
ListenAddress 192.168.XXX.YYY
```

```
# Obsługa użytkowników wyłącznie z
sieci lokalnej:
AllowUsers *@192.168.XXX.YY1
*@192.168.XXX.YY2
# albo dla wszystkich komp. w sieci
lokalnej: AllowUsers
*@192.168.XXX.0/24
```

XXX zastępuję końcówką adresu twojej sieci;

YYY zastępuję końcówką adresu IP twojego serwera;

YY1 zastępuję końcówką adresu IP mojego 1 klienta w sieci;

YY2 zastępuję końcówką adresu IP mojego 1 klienta w sieci;

Otwórz port SSH w zaporze sieciowej UFW:

```
sudo ufw allow from 192.168.XXX.0/24
to any port 22 proto tcp
```

Aby to wszystko zadziało bez ponownego uruchamiania sys. na serwerze należy wydać polecenia:

```
sudo systemctl stop ssh.service
sudo systemctl start ssh.service
```

7.3.2 Dla chętnych: ssh-audit

Służy on do badania popr. konf. serwera ssh.

```
sudo apt install ssh-audit
ssh-audit 192.168.XXX.YYY
```

7.4 Instalacja i Konf. Sys. Wersjonowania Git

W d. 2026-04-17, pią. na grupie dyskusyjnej comp.programming zadałem pyt. "Git own server: How To Protect master Branch?". W d. 2026-06-09, wto., oraz w d. 2026-06-14, Lumin Etherlight <lumin@etherlight.link> odp. na mój post. Poniżej przedstawiam spolszczone i uzupełnione jego rozw.

7.4.1 Założenia Serwera Git

Zakładamy że w zespole programistów jest jeden lider i on obsługuje 2 repo: produkcyjne i swoje własne, robocze. Rozwiązanie polega na założeniu na serwerze repo `/var/git/greatcompany/coolproject`, oraz kont dla wszystkich programistów w zespole: leader, john i mira. Następnie dla każdego z nich tworzy się kat. `/var/git/USER/PROJEKT`. Normalnie programiści pracują na własnych repach. Natomiast gdy któryś stwierdzi, że ich kod jest już gotowy listem el. zgłaszają liderowi "merge request". Wtedy lider "dociąga" do swojego repo gałąź master tego programisty co zgłosił "merge request". Wtedy może przejrzeć kod i gdy oceni go pozytywnie, to może wciągnąć wybrany commit, lub wszystkie zmiany z gałęzi PROGRAMISTA/master.

7.4.2 Instalacja git

```
sudo apt install git
```

7.4.3 Tworzenie Kont Programistów Na Serwerze

```
sudo useradd leader
sudo useradd john
sudo useradd mira
```

```
# Przypisanie haseł dostępu:
sudo passwd leader
sudo passwd john
sudo passwd mira
```

```
# Dodanie do grupy git:
sudo groupadd awesomegroup
sudo usermod -aG awesomegroup leader
sudo usermod -aG awesomegroup john
sudo usermod -aG awesomegroup mira
```

```
# Ustawienie kat. domowych:
sudo usermod -d /var/git/leader leader
sudo usermod -d /var/git/john john
sudo usermod -d /var/git/mira mira
```

7.4.4 Tworzenie Kat. z Repo Na Serwerze

```
# Repo produkcyjne:
sudo mkdir -p
/var/git/greatcompany/coolproject
```

```
# Repo lidera:
```

```
sudo mkdir -p
/var/git/leader/coolproject
```

```
# Repo "zwykłych" programistów:
sudo mkdir -p
/var/git/john/coolproject
sudo mkdir -p
/var/git/mira/coolproject
```

```
# Tworzenie nowych repo na serwerze:
cd /var/git/greatcompany/coolproject
sudo git init --bare
cd /var/git/leader/coolproject
sudo git init --bare
cd /var/git/john/coolproject
sudo git init --bare
cd /var/git/mira/coolproject
sudo git init --bare
```

```
# Nadanie praw dostępu:
sudo chown -R leader:awesomegroup
/var/git
sudo chown -R leader:awesomegroup
/var/git/greatcompany/coolproject
sudo chown -R leader:awesomegroup
/var/git/leader/
sudo chown -R john:awesomegroup
/var/git/john/
sudo chown -R mira:awesomegroup
/var/git/mira/
```

```
# Odczyt dla grupy:
sudo chmod -R g+rx-w /var/git
```

```
# Brak praw dla reszty:
sudo chmod -R o-rwx /var/git
```

```
# Aut. dziedziczenie grupy przez nowe
# pliki w kat.:
sudo find /var/git -type d -exec chmod
g+s {} \;
```

```
# Dodanie wyjątku bezpieczeństwa z
# powodu dostępu do cudzego kat. w
# grupie:
sudo git config --system --add
safe.directory
/git/greatcompany/coolproject
sudo git config --system --add
safe.directory /git/leader/coolproject
sudo git config --system --add
safe.directory /git/john/coolproject
sudo git config --system --add
safe.directory /git/mira/coolproject
```

```
# To w celu skrótu adresów URL:
sudo ln -s /var/git /git
```

7.4.5 Schemat Pracy z Serwerem Git

7.4.5.1 Tworzenie Nwego Repo Produkcyjnego Na Kompie Lidera

```
mkdir coolproject-prod
cd coolproject-prod
git init
```

```
git remote add origin
ssh://leader@192.168.xxx.yyy/git/great
company/coolproject
```

```
git remote add leader
ssh://leader@192.168.xxx.yyy/git/leader/coolproject
```

7.4.5.2 Tworzenie Nowego Lokalnego Repo Git Na Kompie Lidera

```
mkdir coolproject-prod
cd coolproject-prod
git init
git add .
git commit -am "Pierwszy commit!"
```

```
git remote add origin
ssh://leader@192.168.xxx.yyy/git/leader/coolproject
```

```
git remote add john
ssh://leader@192.168.xxx.yyy/git/john/coolproject
```

```
git remote add mira
ssh://leader@192.168.xxx.yyy/git/mira/coolproject
```

Następnie wypchnij zaw. repo:

```
git push
# Lub za 1. razem:
git push --set-upstream origin master
```

7.4.5.3 Pobieranie Repo Na Kompa "Zwykłego" Programisty John

```
git clone ssh://john@192.168.XXX.YYY
:/git/leader/coolproject
```

```
cd coolproject
```

```
# Przełączenie do użycia repo john na
# serwerze:
git remote set-url origin
ssh://john@192.168.20.24/git/john/cool
project
```

```
# Dodanie repa leader jako źródło:
git remote add leader
ssh://john@192.168.xxx.yyy/git/leader/coolproject
```

Podobnie dla miry i ew. reszty programistów.

7.4.5.4 Praca Na Kompie "Zwykłego" Programisty John

Dociąganie zmian z gałęzi gł.:

```
git pull leader master
```

Utworzenie nowej gałęzi roboczej:

```
git checkout -b newfeature
```

Po zmianach, po kompilacji i po testach:

```
git pull upstream master
git rebase master
git add .
git commit -am "Treść commit-a."
```

Rebase powoduje aktualizację gałęzi roboczej o zmiany z mastera jakie w między czasie mogły mieć miejsce (bo nad kodem może pracować wielu programistów na raz). Po zrobieniu rebase zmiany z gałęzi master łądzą przed zatwierdzeniami w gałęzi roboczej. Dzięki temu po merge jest porządek.

Na koniec

```
git checkout master
git merge newfeature
git push
```

Wtedy do john musi wysłać list el. do leader, że chce włączyć gałąź eksperyment do gałęzi master.

7.4.5.5 Lider Dociąga john/master

```
# Wciągnięcie gałęzi john/master:
git fetch john
```

```
# Przegląd kodu john:
```

```

git log --graph john/master
git log -p john/master

# Wciągnięcie wybranego commit:
git switch master
git cherry-pick HASH_COMMIT_OD_JOHN

# Wciągnięcie wszystkich zmian john:
git switch master
git merge john/master

# Wypychanie zmian lidera na serwer:
git push

# Na koniec prac nad nową wer.
# trzeba zaktualizować repo
# produkcyjne:
cd ~/coolproject-prod
git pull leader master

# Utworzenie gałęzi nowej wer.
# Dzięki niej będzie można dodawać
# w przyszłości łatki komendą
# git cherry-pick HASH_COMMIT
git branch release/v1.1

# Wypychanie zmian na serwer prod.:
git push
# Lub za 1. razem:
git push --set-upstream origin master

```

7.5 Instalacja i Konf. Lustrzanego Repo

Ten roz. jest napisany na podst. art. pt. "How to Setup Local APT Repository Server on Ubuntu 20.04", aut. Pradeep Kumar, pub. w d. 2021-02-03, śro., URL: <https://www.linuxtechi.com/setup-local-apt-repository-server-ubuntu>. Info w tym roz. nie zostały w pełni sprawdzone (nie pobrałem pełnego repo, bo to ponad 500GB danych).

7.5.1 Instalacja Potrzebnych Pakietów

```

sudo apt install -y apache2
sudo apt install -y apt-mirror

sudo systemctl enable apache2

```

7.5.2 Przygotowanie Kat. z Lustrzanym Repo

```

sudo mkdir -p /var/www/html/ubuntu
sudo chown www-data:www-data
/var/www/html/ubuntu

```

7.5.3 Konf. apt-mirror

```

sudo cp /etc/apt/mirror.list
/etc/apt/mirror.list-bak
sudo nano /etc/apt/mirror.list

```

Wklej to:

```

##### config #####
set base_path      /var/www/html/ubuntu
set nthreads       20
set _tilde          0
##### end config #####
deb http://archive.ubuntu.com/ubuntu
focal main restricted universe
multiverse
deb http://archive.ubuntu.com/ubuntu
focal-security main restricted
universe multiverse
deb http://archive.ubuntu.com/ubuntu
focal-updates main restricted universe
multiverse
clean http://archive.ubuntu.com/ubuntu

```

7.5.4 Pobieranie Zdalnego Repo (Tworzenie Lustrzanego Repo)

```

sudo apt-mirror

```

Następnie utwórz skrypt pomocniczy, który pobierze listę błędów (które mają być pomijane przy pracy z lustrzanym repo):

```

nano $HOME/bin/cnf.sh

```

I wklej to:

```

#!/bin/bash
for p in "${1:-focal}"{-,
{security,updates}}\
/
{main,restricted,universe,multiverse};
do >&2 echo "${p}"
wget -q -c -r -np -R "index.html*" \

"http://archive.ubuntu.com/ubuntu/dist
s/${p}/cnf/Commands-amd64.xz"

```

```
wget -q -c -r -np -R "index.html*" \
```

```
"http://archive.ubuntu.com/ubuntu/dist  
s/${p}/cnf/Commands-i386.xz"  
done
```

Następnie pobierz listę błędów (które mają być pomijane przy pracy z lustrzanym repo):

```
chmod 700 $HOME/bin/cnf.sh  
$HOME/bin/cnf.sh  
sudo cp -av archive.ubuntu.com  
/var/www/html/ubuntu/mirror/
```

7.5.5 Przetwórz Stacje Robocze Na Pracę z Lustrzanym Repo

```
sudo nano /etc/apt/sources.list
```

I zamień:

```
http://archive.ubuntu.com/ubuntu
```

na:

```
http://192.168.XXX.YYY/ubuntu/mirror/  
archive.ubuntu.com/ubuntu
```

192.168.XXX.YYY - to oczywiście twój serwer z kopią lustrzaną repo Ubuntu.

7.6 Instalacja i Konf. Demona CUPS z Drukarką USB

W tym roz. opiszę udostępnianie z serwera Ubuntu Server, drukarki podpiętej do niego przez port USB. Wynika to z tego, że w przypadku drukarek sieciowych konf. demona CUPS na serwerze jest zbędna (chyba że ktoś chce drukować z serwera). Sposób instalacji i konf. drukarki zrobiłem wg. wskazówek ChatGPT (OpenAI, model GPT-5.5) z d. 2026-06-10, śro. Ja podłączałem drukarkę Brother MFC-L2752DW przez USB (robiłem to wyłącznie dla celów testowych, bo ma ona również interfejsy sieciowe LAN i WLAN z których korzystam na co dzień).

7.6.1 Instalacja CUPS na serwerze

```
sudo apt install cups cups-client
```

7.6.2 Konf. CUPS na serwerze

Dodaj swojego użytkownika do grupy administracyjnej CUPS:

```
sudo usermod -aG lpadmin $USER
```

Uruchom demona CUPS:

```
sudo systemctl enable --now cups
```

Sprawdź czy demon CUPS działa:

```
systemctl status cups
```

Edytuj:

```
sudo nano /etc/cups/cupsd.conf
```

I zmodyfikuj jego treść:

```
Listen *:631  
WebInterface On  
Browsing On  
BrowseLocalProtocols dnssd
```

```
<Location />  
  Allow all  
</Location>
```

```
<Location /admin>  
  Allow all  
</Location>
```

```
<Location /admin/conf>  
  AuthType Default  
  Require user @SYSTEM  
  Allow all  
</Location>
```

7.6.3 Instalacja Sterownika USB Dla Brother MFC-L2752DW Na Serwerze

Podłącz MFC-L2752DW przez USB i sprawdź, czy została wykryta:

```
lsusb
```

Powinno dać m.in. coś takiego:

```
Bus 001 Device 003: ID 04f9:043a  
Brother Industries, Ltd MFC-L2750DW  
series
```

oraz:

```
lpinfo -v
```

Powinno pojawić się coś podobnego do:

```
direct usb://Brother/MFC-L2750DW
%20series?serial=E79626D0N197641
```

Pobierz i zainstaluj sterownik drukarki:

```
wget
https://download.brother.com/welcome/d
lf006893/linux-brprinter-installer-
2.2.6-0.gz
gunzip linux-brprinter-installer-
2.2.6-0.gz
chmod +x linux-brprinter-installer-
2.2.6-0
sudo ./linux-brprinter-installer-
2.2.6-0 MFC-L2752DW
```

Na pytanie:

```
Will you specify the DeviceURI ?
```

odpowiedz:

```
N
```

7.6.4 Włączenie Współdzielenia w CUPS Na Serwerze

```
sudo cupsctl --share-printers
sudo cupsctl --remote-any
sudo systemctl restart cups
sudo ufw allow from 192.168.XXX.0/24
to any port 631 proto tcp
```

7.6.5 Sprawdzanie Drukarki z Serwera

```
lpstat -p
```

Powinieneś zobaczyć np.

```
printer MFC-L2752DW is idle
```

7.6.6 Sprawdzenie Drukarki z Kompa Klienta

W przeglądarce:

```
http://192.168.XXX.YYY:631/printers
```

192.168.XXX.YYY, to oczywiście twój serwer. Na tej s. WWW powinna być widoczna drukarka:

```
MFC-L2752DW
```

7.6.7 Konf. Dostępu Klienta Do "Usieciowionej" Drukarki USB

```
sudo lpadmin \
-p Brother-MFC-L2750DW
-E \
-v
http://192.168.XXX.YYY:631/printers/MF
CL2750DW \
-m everywhere
```

Wydruk próbny:

```
echo "Test" > test.txt
enscript test.txt -o - | ps2pdf -
test.pdf
lp -d Brother-MFC-L2750DW test.pdf
```

7.7 Instalacja i Konf. Demona Samba

Ten roz. został utworzony z pomocą ChatGPT (OpenAI, model GPT-5.5) w d. 2026-06-10, śro.

7.7.1 Instalacja

```
sudo apt install samba
sudo apt install smbclient # Do testów
systemctl status smb
```

7.7.2 Konf. smb

Utworzenie kat. współdzielonego:

```
sudo mkdir -p /home/samba/public
sudo chown -R jacek-marcin:jacek-
marcin /home/samba/public
sudo chmod -R 775 /home/samba/public
```

Udostępnienie kat. współdzielonego:

```
sudo nano /etc/samba/smb.conf
```

Wklej, np.:

```
[Public]
  path = /home/samba/public
  browseable = yes
  read only = no
  guest ok = no
  valid users = jacek-marcin
  create mask = 0664
  directory mask = 0775
```

Znaczenie:

path – udostępniany katalog;

browseable = yes – udział widoczny w sieci;

read only = no – możliwość zapisu;

guest ok = no – wymagane logowanie;

valid users – użytkownicy mający dostęp;

Utworzenie hasła (samba ma osobne hasła):

```
sudo smbpasswd -a jacek-marcin
```

Otworzenie portu w zaporze sieciowej:

```
sudo ufw allow from 192.168.XXX.0/24
to any port 137 proto udp
sudo ufw allow from 192.168.XXX.0/24
to any port 138 proto udp
sudo ufw allow from 192.168.XXX.0/24
to any port 139 proto tcp
sudo ufw allow from 192.168.XXX.0/24
to any port 445 proto tcp
```

Restart demona samby:

```
sudo systemctl restart smbd
```

7.7.3 Testy smbd

Spr. czy porty samby są osiągalne:

```
nmap -p 139,445 192.168.XXX.YYY
```

Spr. czy działa konsola samby:

```
smbclient //192.168.XXX.YYY/Public -U
jacek-marcin
```

Otwiera konsolę w której działają nast. polecenia:

```
ls                # lista plików
cd katalog
get plik.txt      # pobranie pliku
put plik.txt      # wysłanie pliku
```

```
exit
```

Natomiast pod Windows wystarczy:

```
\\192.168.XXX.YYY\Public
```

7.7.4 Montowanie Dysków Samby:

```
sudo apt install cifs-utils
```

Utworzenie lokalnego kat. do którego będziemy montować zdalny dysk:

```
sudo mkdir /mnt/public
```

Zamontowanie dysku:

```
sudo mount -t cifs
//192.168.XXX.YYY/Public /mnt/public -
o username=jacek-marcin
```

Sprawdzenie:

```
ls /mnt/public
```

7.8 Demon NFS

Nie widzę sensu opisywania konf. NFS z nast. powodów:

1. Nie ma prostego mechanizmu kontroli dostępu;
2. Ma problemy z właścicielami kat. i plików (bo opiera się na nr GID i UID, a nie na nazwach);
3. Konf. bezpiecznego połą. z użyciem Kerberos jest b. skomplikowana.

Jedyną istotną zaletą NFS są normalne atrybuty plików zgodne z UNIX/Posix, czyli takie jak w sys. op. Linuks.

Tak więc: Używajcie Samby w firmie i w zagrożeniu!

8 Diagnostyka Sys. Op. Linuks³⁶

8.1 memtest86+

Ten roz. został zainspirowany przez odp. Nuno Silva <nunojsilva@invalid.invalid>, w wątku "A small pre-fix checklist for sick Linux boxes", na grupie dyskusyjnej comp.os.linux.misc, z d. 2026-06-09, wto.

Jak coś regularnie się wiesza, to pierwsza rzecz jaką trzeba spr. to pamięć RAM. Do tego służy memtest86+. Normalnie uruchamia się przy starcie komp. w boot menu zamiast sys. op. Linuks. Można też użyć specjalnej dystrybucji ratunkowej typu LiveCD i po nagraniu na patyk USB z niej uruchomić memtest86+.

8.2 uname

Zwraca informacje o sys. op. Np.

```
uname -a
```

Opcja -a znaczy --all czyli wyświetlenie wszystkich opcji.

8.3 dmesg

ChatGPT (OpenAI, model GPT-5.5) z d. 2026-06-11, śro. Poniżej przytoczono wygenerowaną treść:

"[Poniższe polecenie - przyp. JMJ] Wyświetla z dziennika jądra tylko komunikaty dotyczące błędów sprzętowych i problemów z urządzeniami pamięci masowej (NVMe, SATA), w tym błędy I/O, resety urządzeń oraz błędy pamięci ECC i Machine Check Exceptions."

```
dmesg -T | egrep -i 'mce|edac|ecc|i/o  
error|reset|nvme|ata'
```

8.4 etckeeper

Koncepcja etckeeper jest prosta: lokalne repo git w którym trzymamy wszystkie zmiany jakie zachodzą w kat.

³⁶ Do napisania tego roz. zainspirował mnie post pt. "A small pre-fix checklist for sick Linux boxes", aut. TheLastSysop <thelastsysop@dev.null>, na grupie dyskusyjnej comp.os.linux.misc, pub. w d. 2026-06-09, wto.

ustawień sys. op. Linuks, czyli w /etc . Dodatkowo etckeeper zapewnia integrację z apt i z sudo. To tyle na temat teorii. Przyznam, że dla mnie etckeeper to na razie nowość, tak więc zainteresowanym polecam oficjalną s. dok.:

<https://etckeeper.branchable.com/README>

W przyszłości być może znajdzie się tu więcej informacji na temat etckeeper.

8.5 debsums

Wszystkie pakiety jakie pochodzą z repozytoriów APT (oficjalnych i nieoficjalnych) mają sumy kontrolne wszystkich plików jakie zawierają. To powoduje, że przy superszybkich dyskach SSD błyskawicznie można spr. integralność pakietów zainstalowanych w sys. op. Oczywiście pod warunkiem, że intruz pozostawi debsums w spokoju.

```
sudo apt install debsums
```

Ten skaner podaje listę plików jakie uległy zmianie po instalacji. Domyślnie listuje on wszystkie sprawdzane pliki co jest trochę przytłaczające. Wtedy pomagają opcja -s czyli tryb cichy. Dodatkowo warto włączyć spr. plików ustawień (opcja -a), bo domyślnie są one pomijane. Przykładowe wywołanie może być takie:

```
sudo debsums -as
```

8.6 systemctl

Pozwala diagnozować i kontrolować systemd, czyli głównego demona w sys. op. Linuks. Np.

```
systemctl --failed
```

pokaże demony które nie działają mimo prób ich uruchomienia.

8.7 journalctl

Przepytuje dziennik systemd. Np.:

```
journalctl -b -p warning..alert --no-pager
```

-b Ogranicza komunikaty do bieżącej sesji.

```
journalctl -b -1 # poprzedni boot
```

```
journalctl -b -2 # dwa uruchomienia temu
```

-p warning..alert

Filtruje komunikaty według priorytetu. Poziomy (od najpoważniejszych):

Wartość	Nazwa
0	emerg
1	alert
2	crit
3	err
4	warning
5	notice
6	info
7	debug

--no-pager powoduje, że nie uruchamia prog. less, tylko wypisuje wyniki na konsolę.

8.8 Diagnoostyka Dysków w Sys. Op. Linuks

8.8.1 efibootmgr

ChatGPT (OpenAI, model GPT-5.5) z d. 2026-06-11, śro. Poniżej przytoczono wygenerowaną treść:

"[Poniższe polecenie - przyp. JM]] Wyświetla szczegółową listę wpisów rozruchowych UEFI zapisanych w pamięci NVRAM oraz ich kolejność i ścieżki do plików EFI."

efibootmgr -v

8.8.2 smartctl

ChatGPT (OpenAI, model GPT-5.5) z d. 2026-06-11, czw. Poniżej przytoczono wygenerowaną treść:

"[Poniższe polecenie - przyp. JM]] Wyświetla pełny raport diagnostyczny SMART dla dysku /dev/sdX, zawierający informacje o stanie zdrowia dysku, jego parametrach pracy, historii błędów oraz wynikach testów diagnostycznych."

Z polecenia lsblk dowiesz się jakie masz dyski w sys.

sudo smartctl -a /dev/sdX

X - to litera dysku a, b, c itd.

lub w przypadku dysków NVME:

sudo smartctl -a /dev/nvme0nX

Pow. 0 to nr kontrolera, a X to nr przestrzeni (czyli dysku) i może to być 1, 2, 3 itd.

8.8.3 df

Disk free, więc chyba wszystko jasne. Np.:

df -h

Przełącznik -h powoduje, że lepiej są wyśw. wielk. wolnego miejsca, np. MB, albo GB.

8.8.4 lsblk

Wypisuje urządzenia blokowe w sys. op. Linuks. Np.:

lsblk -f

Wyświetli wszystkie urządzenia blokowe, a opcja -f wypisuje dodatkowo info o sys. plików, etykiety LABEL i UUID.

8.9 Naprawa Dysków w Sys. Op Linux

Pomysł na ten roz. podsunął mi "głos w szumach" jaki przedstawia się agent "Łukasz Niewiadomski" ze SP nr 3 w Pruszczu Gd. z kl. 3A.

Ten roz. w całości został wygenerowany przez ChatGPT (OpenAI, model GPT-5.5) w d. 2026-06-11, czw., po zadaniu pyt. "Linux: Jak standardowo używa się fsck?". Poniżej przytoczono wygenerowaną treść (jednak była ona edytowana przez JM] tak by miała ona bardziej logiczną kol., by pominąć zbędne fragmenty, oraz by poprawić błędy stylistyczne):

"Standardowe użycie fsck zależy od sytuacji, ale najczęściej wygląda ono tak:

8.9.1 Ważne [Naprawiamy Wył. Dyski Niezamontowane - przyp. JM]]

- **Nie należy uruchamiać fsck na zamontowanym systemie plików, zwłaszcza w trybie zapisu, ponieważ może to doprowadzić do uszkodzenia danych.**
- *Dla niektórych systemów plików obowiązują inne zasady:*

- **ext2/ext3/ext4** — `fsck.ext4` wykonuje rzeczywistą kontrolę i naprawę.
- **XFS** — używa się `xfs_repair`; zwykły `fsck` tylko informuje, że naprawa powinna być wykonana innym narzędziem.
- **Btrfs** — zwykle korzysta się z `btrfs scrub`, a `btrfs check --repair` stosuje się ostrożnie.

Najbardziej typowe użycie w praktyce administracyjnej to:

```
sudo umount /dev/sdXN
sudo fsck -f /dev/sdXN
```

a w przypadku automatycznej naprawy:

```
sudo fsck -fy /dev/sdXN
```

gdzie X oznacza dysk, a N numer partycji.

8.9.2 Sprawdzenie Systemu Plików Niezamontowanej Partycji

```
sudo fsck /dev/sda1
```

`fsck` wykryje typ systemu plików i uruchomi odpowiednie narzędzie (np. `fsck.ext4`, `fsck.xfs`, `fsck.fat`).

8.9.3 Automatyczna Naprawa Znalezionych Błędów

```
sudo fsck -y /dev/sda1
```

Opcja `-y` automatycznie odpowiada „tak” na wszystkie pytania o naprawę.

8.9.4 Wymuszenie Pełnego Sprawdzenia

```
sudo fsck -f /dev/sda1
```

Nawet jeśli system plików jest oznaczony jako „czysty”, zostanie sprawdzony.

8.9.5 Typowy Sposób [Postępowania - przyp. JM]] Podczas Problemów z Systemem

1. Uruchomić komputer z Live USB lub w trybie ratunkowym.
2. Upewnić się, że sprawdzana partycja nie jest zamontowana:

```
mount | grep sda1
```

3. Jeśli jest zamontowana, odmontować ją:

```
sudo umount /dev/sda1
```

4. Uruchomić:

```
sudo fsck -f /dev/sda1
```

8.9.6 Sprawdzenie Wszystkich Systemów Plików z /etc/fstab

```
sudo fsck -A
```

Opcja `-R` pozwala pominąć system plików główny:

```
sudo fsck -AR
```

"

8.10 Diagnostyka Sieci w Sys. Op. Linuks³⁷

cytat: "For your diagnostic chapters, I would suggest keeping one warning in big letters: DO NOT START BY REINSTALLING THINGS AT RANDOM. Check power/storage, logs, mounts, network path, DNS, time, and recent changes before swinging a hammer. It saves both uptime and pride."

, źródło: "Re: A small pre-fix checklist for sick Linux boxes", aut. TheLastSysop <thelastsysop@dev.null>, pub. w d. 2026-06-10, śro., na grupie dyskusyjnej comp.os.linux.misc .

³⁷ Do napisania tego roz. zainspirował mnie post pt. "A small pre-fix checklist for sick Linux boxes", aut. TheLastSysop <thelastsysop@dev.null>, na grupie dyskusyjnej comp.os.linux.misc, pub. w d. 2026-06-09, wto.

W tł. przez ChatGPT (OpenAI, model GPT-5.5) w d. 2026-06-10, śro. Poniżej przytoczono wygenerowaną treść:

„W rozdziałach poświęconych diagnostyce sugerowałbym umieścić jedno ostrzeżenie dużymi literami: NIE ZACZYNAJ OD LOSOWEGO PRZEINSTALOWYWANIA RÓŻNYCH RZECZY. Najpierw sprawdź zasilanie i pamięć masową, logi, zamontowane systemy plików, ścieżkę sieciową, DNS, czas systemowy oraz ostatnio wprowadzone zmiany, zanim sięgniesz po młotek. To pozwala uniknąć niepotrzebnych przestojów i oszczędza wstępu.”

8.10.1 ip

Aby wyśw. adresy IP przypisane do każdej karty sieciowej:

```
ip addr
```

Aby wyświetlić reguły trasowania pakietów:

```
ip route
```

8.10.2 whois

To polecenie zwraca info na temat aktualnego dzierżawcy danej domeny. Np.

```
whois wp.pl
[...]
REGISTRAR:
AZ.pl Sp. z o.o.
ul. Zbożowa 4
70-653 Szczecin
Polska/Poland
Tel: +48.914243780
https://az.pl/
domena@az.pl
[...]
```

8.10.3 dig

To polecenie pozwala spr. na jakie adresy IP kieruje dana domena. Np.

```
dig ubuntu.com
[...]
;; ANSWER SECTION:
ubuntu.com.        60      IN
A      185.125.190.20
ubuntu.com.        60      IN
A      185.125.190.21
```

[...]

8.10.4 resolvectl

```
resolvectl status
```

Wyświetla m.in.:

- serwery DNS dla poszczególnych interfejsów;
- domeny wyszukiwania;
- czy używane są DNS-over-TLS, LLMNR, mDNS;
- globalne ustawienia DNS.

8.10.5 ss

```
sudo ss -tulpn
```

Gdy uruchmisz ss bez sudo nie zobaczysz nazw prog.!

służy do wyświetlenia gniazd sieciowych (socketów), na których nasłuchują lub działają procesy w systemie.

ss (socket statistics) jest nowocześniejszym i szybszym następcą netstat.

- -t — pokaż gniazda TCP
- -u — pokaż gniazda UDP
- -l — pokaż tylko gniazda nasłuchujące (listening)
- -p — pokaż proces, który używa gniazda
- -n — nie tłumacz nazw (portów i adresów) na nazwy symboliczne

8.10.6 tcpdump

Do monitorowania ruchu sieciowego służy monitor tcpdump. Wywołuje się go:

```
sudo tcpdump
```

Jednak gdy chcesz zobaczyć tylko nowe połączenia, należy użyć opcji pokazujące tylko pakiety IP/TCP z flagą SYN:

```
sudo tcpdump 'tcp[tcpflags] & (tcp-syn) != 0'
```

Gdy chcesz monitorować tylko rozpoczęcie i kończenie połączeń trzeba dodać flagę FIN:

```
sudo tcpdump 'tcp[tcpflags] & (tcp-syn|tcp-fin) != 0'
```

tcpdump jest świetnym prog., ale wyświetla nieczytelne komunikaty. Jednak ma w sobie zabezpieczenie³⁸ by nie mógł działać w skryptach (dzięki którym można by go "ładnie opakować").

8.10.7 arp-scan

Prog. ten wykrywa urządzenia w sieci lokalnej (kompy, drukarki, serwery, routery itd.)

Najpierw wybierz jedną z kart sieciowych:

ip link

Potem uruchom skanowanie:

```
sudo arp-scan --
interface=TWOJA_KARTA_SIECIOWA
192.168.XXX.0/24
```

8.10.8 nmap

Służy do skanowania otwartych portów oraz wykrywania sys. op. na wybranym kompie. Np.

```
sudo nmap -O -n 192.168.XXX.YYY
```

Skanuje pierwsze 1024 porty (są one przypisane standardowym demonom sieciowym w sys. op. Linuks), a opcja -O dodatkowo stara się wyryć sys. op. hosta 192.168.XXX.YYY.

8.10.9 Tab.: Skanery Sieciowe

Wymienimy tu narzędzia do skanowania komp. w sieci z krótkim opisem. Tak byś mógł wiedzieć czego szukać w razie potrzeby.

Skaner	Zastosowanie
nmap	Rozpoznawanie sys. operacyjnego zdalnych komp. Wykrywanie otwartych portów.
xprobe	Rozpoznawanie sys. operacyjnego zdalnych komp.

³⁸ Podobne zabezpieczenie przed użyciem w skryptach ma prog. **pdfgrep** i **atrm** (do usuwania zadań z **anacron**). Co ciekawe zadania do **anacron** poleceniem **at** można dodawać ze skryptów.

p0f ³⁹	<ul style="list-style-type: none"> ● Rozpoznawanie sys. operacyjnego zdalnych komp.; ● Wykrywanie obecności firewall i NAT; ● Wykrywanie obecności load balancer; ● Wykrywanie odległości od zdalnego komp.; ● Wykrywanie czasu pracy zdalnego hosta.
knocker	Rozpoznawanie sys. operacyjnego zdalnych komp. Wykrywanie otwartych portów.
isic	Tester integralności stosu IP/TCP.
hping2	<ul style="list-style-type: none"> ● Testowanie firewall; ● Zaawansowane skanowanie protów; ● Testowanie sieci różnymi protokołami; ● Wykrywanie MTU; ● Zaawansowane traceroute (różnymi protokołami); ● Rozpoznawanie sys. operacyjnego zdalnych komp.; ● Wykrywanie czasu pracy zdalnego hosta; ● Tester integralności stosu IP/TCP; ● Przydatne narzędzie edukacyjne do nauki protokołu IP/TCP.
icmpush	Pozwala generować własne pakiety ICMP.
nbtscan	Skanowanie usług SMB i NetBIOS (Windws).

³⁹ Co ciekawe jest to prog. Amerykanina polskiego pochodzenia.

fragrouter	Przechwytywanie i modyfikacja ruchu w sieci. Prog. wydaje się niepraktyczny gdy HUB LAN (kablowne) wyszły z użycia (zastąpiły je router z wbudowanymi switch LAN (kablowne) i WLAN (radiowe)).
strobe (pakiet netdiag)	Wykrywanie otwartych portów.
irpas	Zestaw programów: <ul style="list-style-type: none"> ● ass: autonomiczny skaner sys.; ● cdp: generator pakietów; ● file2cable: wrzuca plik w sieć jako ramkę IP/TCP; ● igrp: wstrzykuje pakiety do przestarzałego protokołu trasowania IGRP; ● irdpresponder: wysyła pakiety irdpresponder; ● itrace: podobny do traceroute używa ICMP echo; ● tctrace: podobny do traceroute używa TCP SYN.

9 Ręczna Diagnostyka Bezpieczeństwa

9.1 Testy Zapory Sieciowej

Jak już skończysz konfigurację sys. i podłączysz go do sieci można wykonać podstawowe testy zapory: blokadę skanowania portów i blokadę dostępu do nie otwartych portów.

Testy te wymagają drugiego komp. w tej samej sieci lokalnej.

9.1.1 Test Skanowania Portów

Po pierwsze należy ustalić adres ip twojego komp.

Na nowo zainstalowanym sys. op. Linuks wywołaj:

```
ip a
```

Interesuje cię linia w stylu:

```
inet 192.168.XXX.YYY/24 brd
192.168.XXX.255 scope global
noprefixroute ID_KARTY_SIECIOWEJ
```

To co za inet i przed /24, czyli 192.168.XXX.YYY (oczywiście zamiast XXX.YYY będą konkretne numery) to właśnie aktualny Internet adres karty sieciowej.

Wcześniej w roz. nmap poznaliśmy metodę przeskanowania pierwszych 1024 portów na wybranym kompie. Teraz możemy pójść krok dalej i przeskanować wszystkie porty jest ich $2^{16} - 1$, czyli 65535. Aby je przeskanować użyj polecenia:

```
sudo nmap -O -p- -n 192.168.20.24
```

-O wykrywa OS - jw.;

-p- to pełne skanowanie 65535 portów;

-n Zabrania nmap odwołań do DNS, co przyspiesza skanowanie.

9.1.2 Test Dostępu Do Otwartego Portu Zablokowanego Przez UFW

Blokadę portów sprawdzimy stawiając na nowym sys. op. Linuks z zaporą sieciową UFW testowy serwer WWW na zablokowanym porcie i próbując się do niego łączyć z drugiego komp. Na twoim nowym sys. op. Linuks uruchom:

```
python3 -m http.server 1234
```

Natomiast na drugim komp. wywołaj polecenie:

```
telnet 192.168.XXX.YYY 1234
```

Gdy jest ok możliwe są 2 rezultaty:

1. Polecenie powinno zakończyć się błędem przekroczenia czasu (deny):

```
Connecting to 192.168.XXX.YYY:1234...
failed: Connection timed out.
Retrying.
```

2. Polecenie powinno zakończyć się błędem odmowy dostępu (reject):

```
Trying 192.168.XXX.YYY...
telnet: Unable to connect to remote
host: Connection refused
```

9.2 Skaner Lynis (Skaner Bezpieczeństwa)

Lynis to rozszerzalne narzędzie do kontroli bezpieczeństwa sys. komp. z sys. op. Linux, FreeBSD, macOS, OpenBSD, Solaris i innymi pochodnymi Uniksa.⁴⁰

9.2.1 Instalacja

```
sudo apt install lynis
```

9.2.2 Skanowanie

```
sudo lynis audit system
```

9.2.3 Interpretacja Wyników

```
$ sudo cat /var/log/lynis-report.dat |
grep suggestion | most
suggestion[]=BOOT-5122|Set a password
on GRUB boot loader to prevent
altering boot configuration (e.g. boot
in single user mode without
password)|-|-|
suggestion[]=BOOT-5264|Consider
hardening sys. services|Run
'/usr/bin/sys.d-analyze security
SERVICE' for each service|-|
suggestion[]=KRNL-5820|If not
required, consider explicit disabling
of core dump in
/etc/security/limits.conf file|-|-|
suggestion[]=PROC-3614|Check process
listing for processes waiting for IO
requests|-|-|
suggestion[]=AUTH-9229|Check PAM
configuration, add rounds if
applicable and expire passwords to
encrypt with new values|-|-|
suggestion[]=AUTH-9230|Configure
minimum encryption algorithm rounds in
/etc/login.defs|-|-|
suggestion[]=AUTH-9230|Configure
maximum encryption algorithm rounds in
/etc/login.defs|-|-|
suggestion[]=AUTH-9262|Install a PAM
module for password strength testing
like pam_cracklib or pam_passwdqc|-|-|
[...]
```

Ciekawą opcją Lynis-a jest możliwość uzyskania szczegółowych informacji na temat danego testu.

⁴⁰ <https://en.wikipedia.org/wiki/Lynis>

Przykładowo polecenie:

```
$ sudo lynis show details BOOT-5122
2020-07-05 20:01:21 Performing test ID
BOOT-5122 (Check for GRUB boot
password)
2020-07-05 20:01:21 Found file
/boot/grub/grub.cfg, proceeding with
tests.
2020-07-05 20:01:21 Test: check if we
can access /boot/grub/grub.cfg
(escaped: /boot/grub/grub.cfg)
2020-07-05 20:01:21 Result: file is
owned by our current user ID (0),
checking if it is readable
2020-07-05 20:01:21 Result: file
/boot/grub/grub.cfg is readable (or
directory accessible).
2020-07-05 20:01:21 Result: did not
find hashed password line in this file

2020-07-05 20:01:21 Result: File
'/boot/grub/custom.cfg' does not exist

2020-07-05 20:01:21 Found file
/etc/grub.d/00_header, proceeding with
tests.
2020-07-05 20:01:21 Test: check if we
can access /etc/grub.d/00_header
(escaped: /etc/grub.d/00_header)
[...]
```

9.3 Skaner Rkhunter (Poszukuje Rotkitów)

rkhunter jest skanerem root kitów. Rootkit-y to prog. umieszczane na komp. ofiary celem pełnej kontroli nad nim (np. do kopania krypto-walut, albo ataków na inne komp.).

9.3.1 Instalacja

```
sudo apt install rkhunter
```

9.3.2 Aktualizacja

```
sudo rkhunter --propupd
```

9.3.3 Skanowanie

```
sudo rkhunter --check
```

9.3.4 Interpretacja wyników

```
sudo cat /var/log/rkhunter.log | grep
-e 'Warning' | most
[11:51:46] /usr/bin/lwp-request
[ Warning ]
[11:51:46] Warning: The command
'/usr/bin/lwp-request' has been
replaced by a script: /usr/bin/lwp-
request: Perl script text executable
[11:54:06] Checking for suspicious
(large) shared memory segments
[ Warning ]
[11:54:06] Warning: The following
suspicious (large) shared memory
segments have been found:
[11:55:14] Checking for passwd file
changes [ Warning ]
[11:55:14] Warning: User 'test' has
been removed from the passwd file.
[11:55:14] Checking for group file
changes [ Warning ]
[11:55:14] Warning: Group 'test' has
been removed from the group file.
[11:55:14] Checking if SSH protocol
v1 is allowed [ Warning ]
[11:55:14] Warning: The SSH and
rkhunter configuration options should
be the same:
```

9.4 Skaner Debsecan (Poszukuje exploit-ów)

Exploit – prog. mający na celu wykorzystanie istniejących błędów w oprogramowaniu.⁴¹

9.4.1 Instalacja

```
sudo apt install debsecan
```

9.4.2 Skanowanie i Interpretacja Wyników

```
sudo debsecan | grep -e 'medium
urgency\|high urgency' | most
```

Może się zdarzyć, że nasz sys. jest na tyle czysty, że to polecenie nic nie zwróci.

Gdy nas to nie satysfakcjonuje można użyć polecenia:

41 <https://pl.wikipedia.org/wiki/Exploit>

```
$ sudo debsecan | grep -e 'low
urgency' | most
```

```
CVE-2012-6655 accountsservice (low
urgency)
CVE-2016-1585 apparmor (low urgency)
CVE-2016-1585 apparmor-utils (low
urgency)
CVE-2018-10910 bluez (low urgency)
CVE-2018-10910 bluez-cups (low
urgency)
CVE-2018-10910 bluez-obexd (low
urgency)
CVE-2020-5291 bubblewrap (low urgency)

CVE-2016-2781 coreutils (low urgency)
CVE-2020-12802 fonts-opensymbol (low
urgency)
CVE-2020-12803 fonts-opensymbol (low
urgency)
CVE-2019-14855 gnupg1 (low urgency)
CVE-2019-14855 gnupg1-l10n (low
urgency)
CVE-2019-9904 graphviz (low urgency)
CVE-2019-11470 imagemagick (low
urgency)
[...]
```

9.5 Skaner Fail2ban (Pokazuje Nieudane Próby Logowania)

Jest to skaner poszukujący w logach nieudanych prób logowania na udostępniane usługi (np. SSH). Jednak tutaj pominię ten temat z uwagi na:

- Opis konfiguracji serwera sys. op. Linuks jest poza zakresem tej monografii,
- Z SSH należy pracować w oparciu o klucze a nie hasła (logowanie oparte na hasłach blokuje w rozdziale opisującym konfigurację SSHD).

Więcej o fail2ban np. tu: <https://linuxize.com/post/install-configure-fail2ban-on-ubuntu-20-04/>

10 Automatyzacja Monitorowania Bezpieczeństwa

Kiedyś była "wypasiona", francuska dystrybucja sys. op. Linuks, Mandrake/Mandriva, która miała taki bajer i np. informowała w czasie rzeczywistym np. o skanowaniu portów przez intruza.

Kiedyś bardzo się zdziwiłem jak dostałem na pulpit ostrzeżenie, że z komp. mojej macochy ktoś dokonuje skanowania portów mojej stacji roboczej. Nie muszę dodawać, że moja macocha nie ma nawet pojęcia jak włączyć/wyłączyć sieć w swojej Windzie, tak więc skanowanie portów było i jest poza jej zasięgiem.

Nie wiem nic by w Ubuntu były jakieś prog. monitorujące podejrzany ruch sieciowy. Jednak sam opracowałem skrypty monitorujące sieć:

10.1 Monitorowanie II. Wywołań Prog. i Skryptów

Normalnie sys. Ubuntu nie zlicza il wywołań prog., ale można uruchomić taki monitoring:

```
sudo apt install acct
sudo systemctl enable --now acct
```

Wtedy by wyświetlić il. wywołań wystarczy:

```
sa --sort-num-calls | less
```

11 Skryte Korzystanie z Sys. Op. Linuks

11.1 Skrypt Czyszczący

Należy sobie zaprogramować skrypt czyszczący by choć częściowo automatyzować utrzymanie porządku na kompie.

Czyścić należy:

- Zaostrzyć prawa dostępu do kat. i plików użytkownika, co podałem w roz. Zaostrz Prawa Dostępu Do Katalogów Użytkowników;
- Kasować odszyfrowane pliki z hasłami;
- Kasować z \$HOME zbędne kat. i pliki tworzone przez działające prog.;
- Kasować kat. budowania pakietów ze źródeł;
- Czyścić kat. \$HOME/Pobrane
- Kasować kat. \$HOME/.local/share/Trash
- Naprawić plik \$HOME/.config/user-dirs.dir

Programując ten skrypt należy przejrzeć pliki konfiguracyjne w \$HOME/.config, \$HOME/.local oraz pozostałe pliki i kat. zaczynające się kropką w kat \$HOME.

Skrypt czyszczący należy uruchamiać w nocy gdy się śpi. Służy do tego demon cron. Np. by uruchamiać skrypt czyść.sh o 3 rano, należy raz wywołać polecenie:

```
echo "0 3 * * * root
/home/jacek-marcin/bin/czyść.sh" |
sudo tee /etc/crontab
```

12 Skryte Korzystanie z Sieci Internet

12.1 Przeszkody w Skrytym Korzystaniu z Internetu

12.1.1 Przeglądarki Mają Pełen Dostęp Do Kat. Domowych Wszystkich Użytkowników w sys. op. Linuks.

W Ubuntu domyślne prawa dostępu do kat. innego użytkownika są ustawione tak by łatwo można mu było wszystko ukraść. Nawet więcej! Domyślnie jest możli-

wość odczytu kat. domowego wszystkich innych użytkowników.

W tym dok. podaję jak sobie z tym radzić. Oczywiście mówię o zastrzaniu uprawnień użytkownika i użyciu piaskownicy firejail. W normalnej sytuacji wszyscy klienci sieciowi powinni działać w piaskownicy (podobnie jak wiele innych popularnych prog.).

O tym że przeglądarki to trojany zdradza ich zachowanie:

1. Problemem dotyczącym Chrome i FireFox to nie tolerowanie ustawień ulimit (omówionych w tym dok.). ulimit potencjalnie może pomóc w razie ataku typu przepełnienie bufora;
2. Przeglądarka Chromium z kolei jest dystrybuowana w postaci paczek Snap nad których piaskownicą użytkownik nie ma żadnej kontroli, tak więc spokojnie może wysłać w świat cały kat. domowy i to nie tylko twój ale też wszystkich innych użytkowników z twojego sys. op. Linuks (jw.);
3. Inny znany problem dotyczy przeglądarki WaterFox, która ma zabezpieczenia przed pracą w piaskownicy firejail. Czyli też może robić co jej twórcom się podoba.

Tak więc cała gadka o ciągłym łataniu przeglądarek jest tylko hype (legendą dla frajerów), bo łatanie to tylko pierwszy poziom obrony.

Natomiast twórcy przeglądarek b. starają się unieвозмоić kontrolę użytkownika nad przeglądarkami.

12.1.2 Wysyłanie ID Sys. Op. i ID Przeglądarki

Przeglądarka WWW łącząc się z serwerem WWW zawsze wysyła przez protokół HTTP(S) ID sys. op. i ID samej przeglądarki.

Normalnie jedyną inf. wysyłaną do serwera WWW powinien być j. w jakim ma być zwrócona s. HTML.

Normalnie w „przeglądarkach bez śledzenia” czyli Chromium, Waterfox lub Firewolf powinny mieć wtyczkę która powinna pozwalać na pełną edycję danych identyfikacyjnych, oraz ich maskowanie (wart. stałymi lub losowanymi).

Niestety obecnie (2026 r.) nikt nie chce nawet gadać na ten temat. Pisałem do EFF (d. 2022-04-01, pią.) i na polskich grupach dyskusyjnych (pl.comp.os.linux w d. 2022-04-01, pią.). EFF odp. „Skierujemy sprawę do naszego działu programistycznego.” - jednak do dziś (2024-10-05, sob. nic w tej sprawie nie zrobili). Natomiast na ww grupie odzywali się jedynie „skretyniali agenci wpływu”, którzy histerycznie wrzeszczą że „prywatność, to jedynie kwestia portali społecznościowych”.

Jednak coś z tymi ID można zrobić! Na podst. s. WWW: <https://deviceatlas.com/blog/list-of-user-agent-strings> i <https://whatmyuseragent.com/platforms> można uzyskać listy ID przeglądarek z różnych sys. op. Następnie można napisać skrypty które uruchamiają przeglądarkę Lynx (działa ona w trybie tekstowym) z losowym ID przeglądarki. Podobnie można napisać skrypt uruchamiający wget z losowym ID przeglądarki Mam oba takie skrypty.

12.1.3 Serwery WWW Blokują Klientów Wychodzących z Sieci Tor

Listy adresów serwerów końcowych sieci Tor są publicznie dostępne i są one blokowane przez wiele serwerów WWW.

12.1.4 Dostawcy ISP Publikują Zakresy Swoich Adresów IP

Publicznie są dostępne są bazy adresów IP z podziałem na kraje i operatorów. W normalnym kraju powinno to być tajne, a adresy IP powinny wędrować do kol. op. razem z użytkownikiem (tak jak nr tel.).

Nie trzeba być geniuszem, by stwierdzić, że mając info z 3. pow. p. mamy komplet info na temat kto, gdzie i jak długo siedzi w Internecie.

Więc fakty są takie, że prowadzi się stały monitoring aktywności cywili w sieci.

12.1.5 Dostawcy Internetu Handlują Historią Odwiedzanych s. WWW

Tzw. „zgody maketingowe” – za 5zł.- pozwalają na sprzedaż całej historii odwiedzanych adresów IP i s.

WWW i przych. i wych. nr tel. i SMS. W normalnym kraju powinno to być zabronione.

12.1.6 Brak Manifestów Do s. HTML

Obecnie s. HTML mają linki które zaciągają treści z innych serwerów (niż ten na który wchodzę). Robią to z różnych powodów, np. w celu ładowania skryptów, reklam, albo filmów, a nawet zwykłych obrazków i plików ze stylami CSS. Jest to poważny problem w sytuacji gdy chcemy odblokować jedynie możliwość łączenia z jednym, wybranym serwerem. W praktyce jest to wykonalne jedynie w przypadku wielkich korpo (jak Gogle i Amazon), albo dla amatorskich s. WWW. Żadne komercyjne portale nie publikują wymaganych zakresów IP.

Nawet wikipedia.org przestała publikować listę wymaganych adresów IP. Stało się to wkrótce po moim pyt. Z 2023-01-12, czw. „How to get actual all Wikipedia IP servers list?”. Wtedy grzecznie odpisali mi, cytat:

"Dear Jacek Marcin Jaworski,

While not entirely exhaustive, for most purposes you can use these ranges:

https://www.mediawiki.org/wiki/Wikipedia_Zero/IP_Addresses

Keep in mind, not only do the Wikipedia projects use load balancing, but when only reading a page (not logged in to an account) various CDN's may serve cached pages if you use a service that provides this functionality.

Yours sincerely,

Shaemous Flocks"

, źródło: list el. pt. "Re: [Ticket#2023011210013436] How to get actual all Wikipedia IP servers list?", aut. Wikipedia Volunteer Response Team <info-en@wikimedia.org>, z d. 2023-01-28, sob.

Natomiast 2023-09-28, czw. zauważyłem, że wikipedia.org używa nie zadeklarowanego adresu IP 185.15.59.224. Gdy o to spytałem, odp. mi, cytat

„Dear Jacek Marcin Jaworski,

The Wikipedia Zero project has been retired, we

no longer maintain that list:
https://foundation.wikimedia.org/wiki/Archive:Wikipedia_Zero

Yours sincerely,

Shaemous Flocks"

, źródło: list el. pt. "Re: [Ticket#2023011210013436] How to get actual all Wikipedia IP servers list?", aut. Wikipedia Volunteer Response Team <info-en@wikimedia.org>, z d. 2023-09-28, czw.

Systemowym rozw. tego problemu są manifesty dobrze znane twórcom paczek na sys. Android. Ten manifest powinien zawierać info o adresach jakie są wymagane do prawidłowego działania s. Oprócz tego manifest s. powinien deklarować to czego chce używać s. WWW. Wtedy manifest był by ładowany przed otwarciem s. WWW i możliwe było by spr. jakie wymagania ma dana s. WWW i podjęcie świadomej decyzji czy chce się ją otworzyć czy nie. Wtedy można odblokować w UFW możliwość łączenia z wymaganymi serwerami na czas sesji z serwerem WWW. Można sobie wyobrazić, że przeglądarka może automatyzować cały proces z wyjątkiem kliknięcia przycisku „Otwórz s. WWW” lub „Odrzuć manifest”.

Ponad to z moich doświadczeń wynika, że fałszywy adres wikipedia.pl (nie związany z wikipiedia.org) dokonuje ataków krakerskich.

Dlatego nigdy nie należy używać adresu wikipedia.pl do wchodzenia na pl.wikipedia.org .

12.2 Serwery DNS

Serwery DNS tłumaczą nazwy domenowe takie jak wp.pl albo onet.pl na numery IP. Oczywiście serwerów DNS jest pełno bo ich właścicielom dają dużo informacji o tym co jest popularne w sieci. Kiedyś wierzyłem w większą anonimowość OpenDNS, ale teraz po prostu wybieram najszybsze serwery DNS od Cloudflalre: 1.1.1.1 i 1.0.0.1 . Należy je ustawić konfigurując sieć netplan na każdym kompie w sieci oraz na routerze w sieci lokalnej.

DNSCrypt nie udało mi się uruchomić na Kubuntu 20.04, choć moim zdaniem powinien być domyślnie instalowany i uruchamiany w każdym sys. op.

12.3 Tor Browser

Tor Browser to zmodyfikowana przeglądarka Firefox. Usunięto z niej kod odpowiedzialny za śledzenie i dodano klienta sieci Tor.

Sieć Tor (z którego korzysta Tor Browser) tworzy wirtualną i szyfrowaną podsieć w obrębie sieci Internet i maskuje aktywność rzeczywistego klienta tej sieci (czyli moją stację roboczą). Tak więc jak używam Tor, to mój dostawca Internet nie wie jakie strony odwiedzam. Serwer WWW z jakim się łączę też nie wie skąd się łączę. Jedyne co można podsłuchać, to ruch między końcówką sieci Tor a serwerem WWW z jakim się łączysz (ale tylko wtedy, gdy serwer nie obsługuje https). Działa to tak:

- Uruchamiasz Tor Browser
- Tor Browser wchodzi do wirtualnej, szyfrowanej podsieci Tor;
- Podajesz adres serwera WWW;
- Żądanie dostępu do serwera przechodzi przez sieć Tor;
- Serwer WWW zamiast twojego komp. widzi końcówkę sieci Tor tak jakbyś był w zupełnie innym miejscu na świecie.

W praktyce spec. służby potrafią inwigilować użytkowników sieci Tor (najprawdopodobniej nie jest to wina sieci Tor tylko szpiegostwa telepatycznego). Wiadomo, że amerykańskie sądy posługują się dowodami zebranymi przez te służby.

Przeglądarkę Tor najprościej zainstalować poleceniem:

```
sudo apt install torbrowser-launcher
```

To polecenie instaluje jakiegoś demona Tor a nie samą Przeglądarkę Tor. Moim zdaniem jest to podejrzane.

Dlatego nie zalecam używania pakietu torbrowser-launcher.

tor-launcher przy pierwszym uruchomieniu pobierze i zainstaluje przeglądarkę Tor z oficjalnej strony.

Dlatego lepiej samodzielnie pobrać Przeglądarkę Tor z oficjalnej strony projektu.

Gdy używasz Przeglądarkę Tor w kat. domowym partycja z kat. \$HOME nie może być montowana z flagą noexec (plik /etc/fstab).

Przeglądarkę Tor należy zawsze uruchamiać w piaskownicy firejail.

Wielkie korpo szykanują użytkowników sieci Tor (po prostu odrzucając ruch ze wszystkich końcówek sieci Tor).

Z kolidens używania Przeglądarki Tor na skompromitowanym terminalu podważa fakt, że key-logery to podst. narzędzie szpiegowskie (moim zdaniem wszystko co się wklepuje w sprytne telefony leci od razu do SZAP na serwery Google i dalej do CIA, NSA i reszty).

Trzeba też mieć świadomość, że za korzystanie z Tor złoty pieniążek się należy.

12.4 Poprawa Prywatności w Tor Browser, i w Firefox

Tor Browser to w pełni kompatybilny klon Firefox.

Wszystkie rozszerzenia z Firefox działają w Tor Browser.

Rozszerzenia z Chrome nie działają w Firefox.

Często rozszerzenia mają odrębne wersje dla Chrome i dla Firefox.

12.4.1 Włącz Kasowanie Całej Historii Przy Zamykaniu

12.4.2 Zainstaluj Dodatek [HTTPS Everywhere](#)

Ten dodatek powoduje, że przeglądarka (gdy ma taką możliwość) to faworyzuje szyfrowane połączenia czyli HTTPS.

12.4.3 Zainstaluj Dodatek [Privacy Badger](#)

Ten dodatek monitoruje na stronach reklamy i elementy które mogą Ciebie śledzić i je wyłącza gdy wykryje ich aktywność na 3 różnych stronach WWW.

Privacy Badger nie blokuje reklam tak długo jak one nie usiłują śledzić twoich działań w Internecie.

Po za instalowaniem przeglądarki i jej dodatków należy starannie przejrzeć wszystkie ich opcje.

12.5 Przeglądarka Chromium

Chromium to Chrome bez śledzenia. Czyli Chromium dla Chrome jest tym co Waterfox dla Firefox.

Jest możliwość wejścia do sieci Tor przez Chromium i Chrome ale to wymaga kompilacji pakietu Tor ze źródeł i instalacji odpowiedniej wtyczki⁴².

Aby zainstalować Chromium należy wydać polecenia:

```
sudo snap install chromium
```

Z przeglądarki Chromium nie należy korzystać, bo nie działa ona w piaskownicy firejail (czyli szpieguje użytkowników i kradnie ich dane).

Z przeglądarki Chromium nie należy korzystać, bo brak możliwości wpłacania pieniędzy za jej użycie (czyli ma generować kwity bankowe jakich nie można w żaden normalny sposób spłacić).

12.6 Poprawa Prywatności w Chromium i Chrome

Chromium to w pełni kompatybilny klon Chrome.

W Chromium działają wszystkie rozszerzenia Chrome.

Rozszerzenia z Firefox nie działają w Chrome.

Często rozszerzenia mają odrębne wersje dla Chrome i dla Firefox.

12.6.1 Włącz Kasowanie Całej Historii Przy Zamykaniu

12.6.2 Zainstaluj Dodatek [HTTPS Everywhere](#)

Ten dodatek powoduje, że przeglądarka (gdy ma taką możliwość) to faworyzuje szyfrowane połączenia czyli HTTPS.

⁴² Jest to opisane tu: <https://www.techrepublic.com/article/how-to-install-tor-for-chrome-for-even-more-private-browsing>.

12.6.3 Zainstaluj Dodatek [Privacy Badger](#)

Ten dodatek monitoruje na stronach reklamy i elementy które mogą Ciebie śledzić i je wyłącza gdy wykryje ich aktywność na 3 różnych stronach WWW.

Privacy Badger nie blokuje reklam tak długo jak one nie usiłują śledzić twoich działań w Internecie.

Po za instalowaniem przeglądarki i jej dodatków należy starannie przejrzeć wszystkie ich opcje.

12.6.4 Autouzupełniaj Wyszukiwania i Adresy URL

Wyłącz to na stronie:

```
chrome://settings/syncSetup
```

12.6.5 Ulepsz Wyszukiwanie i Przeglądanie

Wyłącz to na stronie:

```
chrome://settings/syncSetup
```

12.6.6 Wysyłaj Żądanie „Bez Śledzenia” Podczas Przeglądania

Włącz to na stronie:

```
chrome://settings/cookies
```

12.6.7 Kontynuuj Działanie Aplikacji w Tle Po Zamknięciu Chromium

Wyłącz to na stronie:

```
chrome://settings/privacy
```

12.7 Inne Przydatne Dodatki

12.7.1 I don't care about cookies

12.7.1.1 Tor Browser i Firefox

<https://addons.mozilla.org/en-US/firefox/addon/i-dont-care-about-cookies/> ;

12.7.1.2 Chromium i Chrome

<https://chrome.google.com/webstore/detail/i-dont-care-about-cookies/fihnjjciajhdojfnbdddafaoknhlnja> .

12.7.2 Otwieranie Linku i Przejście Do Nowej Karty Jednym Mlaskiem Środkowego Przycisku Pyszy

12.7.2.1 Tor Browser i Firefox

Otwierasz stronę konfiguracji:

`about:config`

I zmieniasz:

`browser.tabs.loadInBackground = true`

na:

`browser.tabs.loadInBackground = false`

12.7.2.2 Chromium i Chrome

Zainstaluj dodatek:

<https://chromewebstore.google.com/detail/tabs-to-front-v2/iiojfiifkpkjkhcdjfgkfmfobhfdohlecg>

12.8 Wyszukiwarki

12.8.1 Brave Sarch

W 2026-05-19, wto. przepytalem ChatGPT (OpenAI, model GPT-5.5) na temat "Jakie obecnie są dostępne płatne wyszukiwarki?". Po jego wypowiedzi zdecydowałem się subskrybować Brave Search za 3\$/mies. Co ciekawe usługę wyszukiwarki Brave Search można opłacić, ale przeglądarki Brave Browser już nie. Jest to tym dziwniejsze, że Brave Search w wer. komercyjnej działa jedynie na Brave Browser. Nie mam pojęcia jak to będzie rozliczone, ale obecnie nie ma innej opcji by normalnie płacić za usługę niezależnej wyszukiwarki.

12.8.2 Google.com

Tu mamy czasem lepsze wyniki wyszukiwania niż w Brave Browser.

Google otwarcie deklaruje maks. szpiegostwo swoich użytkowników.

Mimo, że sieć Internet jest jedna, to każdy użytkownik Google dla tych samych zapytań widzi inne wyniki, bo ta wyszukiwarka cenzuruje i profiluje wyniki dla każdego osobno.

Google szykanuje użytkowników sieci Tor (odrzuca poł. z tej sieci).

Dlatego tej wyszukiwarki należy używać w ostateczności.

12.8.3 Tab.: Porównanie Brave Search i Google.com

ChatGPT (OpenAI, model GPT-5.5) w d. 2026-06-10, śro. Poniżej przytoczono wygenerowaną treść:

<i>Cecha</i>	<i>Brave Search</i>	<i>Google.com</i>
<i>Prywatność</i>	★★★★★	★★☆☆☆
<i>Śledzenie użytkownika</i>	<i>Minimalne</i>	<i>Rozbudowane</i>
<i>Personalizacja wyników</i>	<i>Nieznaczną</i>	<i>Bardzo duża</i>
<i>Wielkość indeksu WWW</i>	<i>Mniejszy</i>	<i>Największy</i>
<i>Trafność wyników ogólnych</i>	<i>Dobra</i>	<i>Bardzo dobra</i>
<i>Wyniki lokalne (firmy, mapy)</i>	<i>Średnie</i>	<i>Doskonałe</i>

Cecha	Brave Search	Google.com
Zakupy, restauracje, mapy	Ograniczone	Bardzo rozbudowane
Reklamy	Mniej nachalne	Dużo reklam
AI w wyszukiwarce	Można wyłączyć	AI Overviews praktycznie zawsze
Własny indeks stron	Tak	Tak
Otwartość algorytmu	Większa (Goggles)	Mała
Szybkość	Bardzo dobra	Bardzo dobra

12.8.4 Tab.: Inne Wyszukiwarki z Własnym Indekssem

ChatGPT (OpenAI, model GPT-5.5) w d. 2026-06-10, śro. Poniżej przytoczono wygenerowaną treść:

Wyszukiwarka	Własny indeks	Uwagi
Google	✓	Największy indeks na świecie
Bing	✓	Microsoft, drugi co do wielkości
Brave Search	✓	Duży nacisk na prywatność
Mojeek	✓	Brytyjska, prywatnościowa
Yandex Search	✓	Bardzo mocna dla rosyjskojęzycznego Internetu
Baidu	✓	Dominuje w Chinach
Yep Search	✓	Rozwijana przez Ahrefs
Kagi Search	częściowo	Własny indeks + wiele źródeł
Stract	✓	Projekt open source
Common Search	✓	Oparty na danych Common Crawl

Obecnie tylko pow. organizacje robią coś poważnego z technicznego p. widzenia w kwestii wyszukiwania w sieci Internet. Reszta wyszukiwarek żeruje na ich dokonaniach.

13 Poczta el.

13.1 Podpisywanie i Szyfrowanie Poczty El.

Okazuje się, że ten temat podjęła fundacja FSF na swojej s. WWW: <https://emailselfdefense.fsf.org/pl>. Zrobili nawet bota Edwarda który pozwala na przetestowanie podpisów el. i szyfrowania poczty el.

13.2 Niezbędna Konf. Klienta Poczтового Thunderbird (w j. ang. Thunderbird)

Thunderbird jest nie wygodny w użyciu. Wynika to oczywiście z faktu, że jest gratisem oraz że jest wer. eksportową. Za patologie w tym prog. odpowiadają projektanci (na podst. <https://www.thunderbird.net/pl/about/>): Jesse Miksic, Laurel Terlesky i Solange Valverde.

13.2.1 Triki Pozwalające Częściowo Uzdrowić Thunerbird

Naprawa Thunerbird jest tylko częściowo możliwa, bo niektóre opcje nie działają tak jak powinny (np. wył. aut. rozwijania drzewa wiad.), a innych po prostu nie wiadomo jak zmienić (np. nie wiem jak zmienić podkreślenie wątku z nowymi wiad. na pogrubienie).

Należy kliknąć hamburger→Ustawienia→Edytor Ustawień (na dole tej zakładki). Wtedy w zakładce „Preferencje zaawansowane” można zmieniać wart. zmiennych:

Sort wiad. na grupach dyskusyjnych wg wiad. otwierającej wątek:

mailnews.sort_threads_by_root na true.

Naprawa zbyt małej czcionki w podglądzie wiad. i w edytorze wiad.:

font.size.monospace.x-unicode na 17

font.size.monospace.x-western na 17

font.name.sans-serif.x-unicode na Noto Sans

font.name.sans-serif.x-western na **Noto Sans**

Wyśw. listów el. jako lista:

mailnews.default_view_flags na **0**

Wyśw. newsów jako drzewo (w wątkach):

mailnews.default_news_view_flags na **1**

Wył. skracania nazw na liście grup dyskusyjnych:

mail.server.default.abbreviate na **false**

Przy używaniu Internetu przez hotspot ze sprytnego tel., który zrywa nieużywane poł. IP/TCP, warto ustawić minimalny czas sprawdzania nowych wiad. tak by wyglądało że poł. ciągle jest używane. Dlatego warto ustawić sprawdzanie wiad. news co 1 min.:

Konfiguracja kont -> TWÓJ_SERWER_NEWS -> Konfiguracja Serwera -> Sprawdzaj, czy nadeszły nowe wiadomości co: 2 minut

Warto też ustawić maks. czasy odp. serwerów news i poczty el.:

news.tcptimeout = 30

mail.server.server1.timeout = 30

mail.server.server3.timeout = 30

Warto też skorzystać z możliwości jakie dają płatne serwery news, czyli wiele jednoczesnych poł., np. news.giganews.com umożliwia do 100 jednoczesnych poł.:

news.max_connections 100

14 Podpisywanie Dok. PDF

Ten roz. był możliwy do napisania dzięki mojemu pyt. na grupie dyskusyjnej pl.comp.os.linux i odp. Arkadiusza 'Black Fox' Artyszuka, w d. 2024-12-13, pią. Wtedy napisał on jak prawidłowo podpisywać dok. PDF prog. GNU gpg. Bo w mojej komendzie brakowało opcji `--not-dash-escaped` - bez niej GNU gpg psuł moje dok. PDF.

Linuks umożliwia nam bezpłatne podpisywanie cyfrowe dok. PDF! Dzięki temu wszystkie wysyłane dok. PDF możemy chronić przed nieautoryzowanymi zmianami, bo wtedy będą one łatwe do wykrycia przez Ciebie i przez odbiorcę. Podpisywanie dok. PDF przydaje się nawet

przy wysyłaniu podań o pracę. Oto sposób na podpisywanie dok. PDF prog. GNU gpg:

Najpierw trzeba zainstalować prog. GNU gpg:

```
sudo apt install gpg
```

Następnie należy wygenerować klucze publiczny i prywatny (oczywiście jest to niekonieczne gdy wygenerowałeś je w p. Podpisywanie i Szyfrowanie Poczty El.):

```
gpg --full-generate-key
```

Następnie odpowiadaj na kol. pyt. Gdy nie jesteś pewien, to zostaw opcję domyślną. Jednak zaznacz rozmiar klucza na 4096. Zalecany czas ważności klucza jest 2 lata. Ważne jest także zabezpieczenie klucza hasłem (nie jest to jakieś super zabezp., bo krakerzy w pierwszej kol. w spenetrowanym sys. instalują keylogery, ale hasło to lepsze niż nic).

Aby wyświetlić listę kluczy należy użyć polecenia:

```
$ gpg --list-keys
```

U mnie zwraca ono taką listę:

```
pub  rsa4096 2024-12-10 [SC] [wygasa:
2031-12-09]
     EBFD1A464130993FBBC230FE221740E87
CE10580
uid  [ absolutne ] Jacek Marcin
Jaworski <jaworski1978@adres.pl>
sub  rsa4096 2024-12-10 [E] [wygasa:
2031-12-09]
```

```
pub  rsa4096 2025-11-09 [SC] [wygasa:
2027-11-09]
     4A541AA7A6E872318B85D7F6A651CC392
44B0BFA
uid  [ absolutne ] Jacek Marcin
Jaworski <jmj@energokod.gda.pl>
sub  rsa4096 2025-11-09 [E] [wygasa:
2027-11-09]
```

Mając klucz można już podpisywać dok. PDF. Robi to kol. komenda konsolowa:

```
gpg --local-user "$gNazwaKlucza" FA --
pinentry-mode=loopback --batch --
passphrase="$gHaslo" --clearsign --
not-dash-escaped --
output="$1PDFPodpisany"
"$1PDFZrodlowy"
```

Aby spr. czy dok. jest prawidłowo podpisany użyj polecenia:

```
gpg --verify "$1PDFPodpisany"
```

Wynik powinien być podobny do poniższego:

```
gpg: Podpisano w pią, 13 gru 2024,
12:19:08 CET
gpg: przy użyciu klucza RSA
EBFD1A464130993FBBC230FE221740E87CE105
80
gpg: Poprawny podpis złożony
przez ,,Jacek Marcin Jaworski ''
[absolutne]
```

15 Komunikacja z Androidem Przez adb

Ten rozdział w całości został wygenerowany przez ChatGPT (OpenAI, model GPT-5.5) w d. 2026-06-12, pią. po zadaniu pyt.: "Linux: Omów sposób łączenia z Androidem przez ADB i podstawowe czynności jakie są dzięki temu możliwe." Poniżej przytoczono wygenerowaną treść (jednak była ona edytowana przez JM) tak by miała ona bardziej logiczną kol., by pominąć zbędne fragmenty, oraz by poprawić błędy stylistyczne):

"ADB (Android Debug Bridge) to narzędzie z pakietu Android SDK umożliwiające komunikację komputera z urządzeniem z Androidem przez USB lub sieć TCP/IP. Działa w systemach Linux, Windows i macOS.

ADB jest przede wszystkim narzędziem dla programistów i administratorów, ale przydaje się także do diagnostyki, automatyzacji, tworzenia kopii plików i zarządzania urządzeniem bez konieczności używania ekranu telefonu.

15.1 Instalacja adb w Linuksie

```
sudo apt install adb
```

15.2 Przygotowanie Telefonu

1. Włącz **Opcje programistyczne**:

- *Ustawienia → Informacje o telefonie → 7 razy kliknij „Numer kompilacji“.*

2. Włącz [w Ustawienia→System→ Opcje programistyczne→ Debugowanie USB - przyp. JM]:

- **Debugowanie USB.**

3. Podłącz telefon przewodem USB.

4. Na ekranie telefonu zaakceptuj komunikat:

Zezwolić na debugowanie USB?

i najlepiej zaznaczyć:

Zawsze zezwalać z tego komputera

15.3 Sprawdzenie Połączenia

Uruchom serwer ADB:

```
adb start-server
```

Wyświetl podłączone urządzenia:

```
adb devices
```

Przykład:

```
List of devices attached
R58N1234567 device
```

Jeżeli widzisz:

```
unauthorized
```

to należy zaakceptować klucz RSA na ekranie telefonu.

15.4 Podstawowe Czynności

15.5 Najczęściej Używane Polecenia [adb - przyp. JMJ]

Polecenie	Funkcja
<code>adb devices</code>	lista urządzeń
<code>adb shell</code>	konsola Androida
<code>adb push</code>	wysłanie pliku
<code>adb pull</code>	pobranie pliku
<code>adb install</code>	instalacja APK
<code>adb uninstall</code>	usunięcie aplikacji
<code>adb logcat</code>	logi systemowe
<code>adb reboot</code>	restart
<code>adb reboot recovery</code>	wejście do recovery
<code>adb tcpip 5555</code>	włączenie ADB przez sieć
<code>adb connect IP:5555</code>	połączenie przez Wi-Fi
<code>adb sideload plik.zip</code>	instalacja ROM-u w recovery

15.6 Wykonywanie Pojedynczych Poleceń

```
adb shell date
adb shell df -h
adb shell getprop
```

Informacje o systemie:

```
adb shell getprop
ro.build.version.release
```

15.7 Powłoka Linuksa w Telefonie

```
adb shell
```

Otrzymujemy konsolę systemu Android:

```
$ uname -a
$ ls /sdcard
$ ps
```

Wyjście:

```
exit
```

15.8 Kopiowanie Plików

15.8.1 Z Telefonu Do Komputera

```
adb pull /sdcard/DCIM/zdjecie.jpg
```

[przykład JMJ:]

```
adb pull
/storage/self/primary/DCIM/Camera/IMG_
20260605_175425_989.jpg
```

lub cały katalog:

```
adb pull /sdcard/DCIM/
```

15.8.2 Z Komputera Do Telefonu

```
adb push film.mp4 /sdcard/Movies/
```

15.9 Lista Aplikacji

```
adb shell pm list packages
```

Filtrowanie:

```
adb shell pm list packages | grep
firefox
```

15.10 Instalowanie Aplikacji APK

```
adb install program.apk
```

Aktualizacja istniejącej aplikacji:

```
adb install -r program.apk
```

Usunięcie aplikacji:

```
adb uninstall nazwa.pakietu
```

Np.:

```
adb uninstall org.mozilla.firefox
```

15.11 Zrzut Ekranu

Na telefonie:

```
adb shell screencap /sdcard/screen.png
```

Pobranie na komputer:

```
adb pull /sdcard/screen.png
```

Można też jednym poleceniem:

```
adb exec-out screencap -p > screen.png
```

15.12 Nagranie Ekranu

```
adb shell screenrecord  
/sdcard/video.mp4
```

Przerwanie nagrywania:

Ctrl+C

Pobranie:

```
adb pull /sdcard/video.mp4
```

Można to zautomatyzować:

```
adb shell screenrecord  
/sdcard/video.mp4 && adb pull  
/sdcard/video.mp4
```

lub:

```
adb shell screenrecord --time-limit 30  
/sdcard/video.mp4 && adb pull  
/sdcard/video.mp4
```

15.13 Sprawdzanie Stanu Baterii

```
adb shell dumpsys battery
```

Przykładowy wynik:

```
Current Battery Service state:  
AC powered: false  
USB powered: true  
Wireless powered: false  
Max charging current: 3000000  
Max charging voltage: 5000000  
Charge counter: 4587000  
status: 2  
health: 2  
present: true  
level: 87
```

```
scale: 100  
voltage: 4210  
temperature: 295  
technology: Li-ion
```

Najważniejsze pola:

- `level: 87` — poziom naładowania [%].
- `temperature: 295` — temperatura 29,5 °C (dziesiąte części stopnia).
- `voltage: 4210` — napięcie 4,210 V.
- `status:`
 - 2 — ładowanie,
 - 3 — rozładowywanie,
 - 5 — pełne naładowanie.
- `health:`
 - 2 — stan prawidłowy,
 - 3 — przegrzana,
 - 4 — uszkodzona,
 - 7 — zimna.

15.14 Rejestrowanie Logów Systemowych

```
adb logcat
```

Filtrowanie:

```
adb logcat | grep Bluetooth
```

Zapis do pliku:

```
adb logcat > log.txt
```

Przydatne przy diagnozowaniu problemów.

15.15 Restart Urządzenia

Normalny:

```
adb reboot
```

Do recovery:

```
adb reboot recovery
```

Do bootloadera:

`adb reboot bootloader`

15.16 Połączenie Przez Wi-Fi

Po podłączeniu USB:

`adb tcpip 5555`

Sprawdzenie adresu IP telefonu:

`adb shell ip addr show wlan0`

Połączenie:

`adb connect 192.168.1.50:5555`

Lista urządzeń:

`adb devices`

Odłączenie:

`adb disconnect`

W nowszych Androidach (11+) możliwe jest parowanie bezprzewodowe:

`adb pair IP:PORT`

15.17 Przekierowanie portów

Udostępnienie portu telefonu na komputerze:

`adb forward tcp:8080 tcp:8080`

Można w ten sposób debugować serwery działające na urządzeniu.

15.18 Dostęp Root

Jeżeli urządzenie jest zrootowane:

`adb root`

oraz:

`adb shell
su`

możliwy jest dostęp do całego systemu plików.

15.19 Czego nie można zrobić bez roota?

Nie można m.in.:

- odczytywać danych innych aplikacji,
- modyfikować plików systemowych,
- usuwać aplikacji systemowych z partycji systemowej,
- zmieniać jądra Linuxa,
- uzyskać pełnego dostępu do /data."

16 Lektura Uzupełniająca i Bibliografia

<https://wiki.debian.org/SetupGuides/SecurePersonalComputer>

<https://wiki.ubuntu.com/BasicSecurity>

<https://www.ncsc.gov.uk/collection/end-user-device-security/platform-specific-guidance/ubuntu-18-04-lts>

<https://www.techrepublic.com/article/how-to-check-for-weak-passwords-on-your-linux-systems-with-john-the-ripper>

<https://securityboulevard.com/2020/08/linux-server-security-10-linux-hardening-security-best-practices>

<https://www.makeuseof.com/linux-hardening-tips-sysadmins>

<https://www.debian.org/doc/manuals/securing-debian-manual/index.en.html>

<https://wiki.debian.org/SetupGuides/SecurePersonalComputer>

<https://linuxize.com/post/how-to-setup-a-firewall-with-ufw-on-ubuntu-20-04>

https://www.reddit.com/r/privacytoolsIO/comments/g31pfm/ubuntu_security_guide

<https://www.maketecheasier.com/secure-newly-installed-ubuntu>

<https://askubuntu.com/questions/579552/how-can-i-have-a-very-secure-ubuntu-desktop-system>

4. Ograniczenia licencji nie dotyczą autora.

Bibliografia

nano-podr-pdf: Chris Allegretta, GNU nano, 2026
inst-ubun-desk-www: Oliver Smith
<oliversmith@canonical.com, Canonical Web Team
<webteam@canonical.com>, Install Ubuntu Desktop -
Ubuntu Desktop documentation, 2026,
<https://documentation.ubuntu.com/desktop/en/latest/tutorial/install-ubuntu-desktop>
idealna-recenzja-linux-mag-pl-2024-05: Hans Georg
Eber, Idealna Recenzja, 2024

17 Podziękowania

W tym miejscu należą się podziękowania dla (kol. chronologiczna):

- Arkadiusz 'Black Fox' Artyszuk
<blackfox_pl@protonmail.com>;
- Mateusz Viste <mateusz@x.invalid>;
- Tomaszek <d3bkowski@gmail.com>;
- Lumin Etherlight <lumin@etherlight.link>;
- TheLastSysop <thelastsysop@dev.null>;
- Nuno Silva <nunojsilva@invalid.invalid>;
- "głos w szumach" jaki przedstawia się agent
"Łukasz Niewiadomski" ze SP nr 3 w Pruszczu
Gd. z kl. 3A.

18 Licencja

Jest to licencja dotycząca tego dokumentu. Pliki wskazywane przez linki mogą być publikowane na innych licencjach. Zasady licencji:

1. **Zezwolenie na kopiowanie** Zezwala się na niekomercyjne kopiowanie tego dokumentu;
2. **Zezwolenie na udostępnianie** Ten dokument można udostępniać (jednak bezpłatnie);
3. **Zabronione modyfikowanie** Tego dokumentu nie można modyfikować ani skracać ani dodawać czegokolwiek.