Zabezp. Sys. Debian-Ubuntu

autor:	**Jacek Marcin Jaworski**
pseudonim:	**Energo Koder Atlant**
pomocnicy autora:	**BRAK**
miejsce:	**Pruszcz Gd., Polska**
utworzono:	**2020-07-12, nie.**
wersja: 5288 z dnia:	**2025-01-18**
program składu:	**Libre Office Writer**
sys. op.:	**Kubuntu, Triskel**

Spis treści

Streszczenie

Niniejsza monografia opisuje następujące zagadnienia dotyczące zabezpieczenia stacji roboczej z sys. Linuks (Debian, Ubuntu i pochodne):

- Budowa sieci Internet;
- Niebezpieczeństwa związane z korzystaniem z sieci Internet;
- Bezpieczeństwo w sieci lokalnej;
- Mechanizmy bezpieczeństwa w sys. Linuks;
- Koncepcja użycia komputera z sys. Linuks działającego w sieci Internet;
- Przygotowania do instalacji sys. Linuks;
- Instalacja sys. Linuks;
- Konfiguracja sys. Linuks po instalacji;
- Konfiguracja sys. Linuks dla programisty
- Konfiguracja sys. Linuks dla nie programisty
- Ręczna diagnostyka bezpieczeństwa sys. Linuks;
- Automatyzacja monitorowania bezpieczeństwa w sys. Linuks;
- Skryte korzystanie z sys. Linuks;
- Skryte korzystanie z sieci Internet.

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

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

O autorze

Programuję komputery od lut. 1997r. Mam tytuł Technika Elektronika spec. Systemy Komputerowe. Zaliczyłem 3 lata studiów informy na PG (jednak dyplomu inż. nie zrobiłem).

W latach 1999-2007 byłem programistą aplikacji w C++ dla sys. Windows. W latach 2018-2022 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 ✷Zdobycie biegłości w pracy z sys. op. Plan9✷

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

Wystrzegam się jak mogę „produktów” wielkich korpo które z niejawnych powodów wynajdują tylko patologiczne wynalazki[1].

Jestem poszukiwaczem i kolekcjonerem "dobrych zasad życiowych" i "dobrych zasad inżynierskich". Dzięki tym zwięzłym, 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.

Skróty

dok.	dokument
el.	element
f.	funkcja
j.	język
kat.	katalog
kol.	kolejny
kom.	komputer
ks.	książka
l.	liczba
łac.	łacina
man	podręcznik (w j. ang. manual)
NPT	protokół synchronizacji czasu (w j. ang. Network Time Protocol)
odp.	odpowiedź.
ost.	ostatni
p.	punkt
pam.	pamięć
PG	Politechnika Gdańska
poł.	połączenie
pow.	powyższy
pyt.	pytanie
s.	strona
sys. op.	system operacyjny
wer.	wersja
wył.	wyłączenie
zaw.	zawartość

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 korpo, 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 Pająk z NZ: W organizacjach pasożytniczych wszystkie złe pomysły pojawiają się od górnie, a wszystkie postępowe koncepcje powstają oddolnie.

Treść tej monografii

Cele tej monografii

1. Stworzenie dobrego, sprawdzonego i szybkiego do wdrożenia przepisu na prawidłową konfigurację stacji roboczej z sys. Linuks w domu i w pracy.

   Prawidłowa konfiguracja zapewnia: bezpieczeństwo, prywatność i wydajność;

2. Stworzenie dobrego, sprawdzonego i szybkiego do wdrożenia przepisu na prawidłową konfigurację sieci domowej;

3. Propagowanie wiedzy o alternatywnych sposobach używania komputerów i sieci.

Wizja

Maksymalne bezpieczeństwo, prywatność i wydajność pracy na komputerze z sys. Linuks.

Strategia

Zero zaufania do: producentów sprzętu, oprogramowania i dostawców usług telekomunikacyjnych.

Taktyka

Blokowanie wszystkiego co zbędne i podejrzane.

Kasowanie wszystkiego co zbędne i podejrzane.

Założenia wstępne

Aby osiągnąć w. postawione cele muszę przyjąć pewne założenia:

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

Grupa docelowa

Grupa docelowa to użytkownicy sys. 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. Linuks - głównie użytkownicy domowi;
- Zawodowi użytkownicy sys. Linuks nie będący administratorami.

Czego nie opisałem w tej monografii

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

Skupiam się na użytkowniku stacji roboczej z sys. Linuks. Opis zabezpieczania serwerów pozostawmy certyfikowanym adminom.

Nie poruszam kwestii usług VPN, bo uważam że tylko spowalniają dostęp do sieci. Bo nie ma co wierzyć, że dostawca VPN „jest niezależny” i wolny od układów 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.

Starałem się opracować jak najlepszą instrukcję zasad pracy z sys. 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. LINUKS PO ZASTOSOWANIU PONIŻSZYCH INSTRUKCJI.

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

2 Czyli nie ma konieczności szyfrowania partycji.
3 W j. ang.: back doors

Forma tej monografii

Słownik pojęć

Na potrzeby tej monografii wprowadzam wygodne skróty myślowe:

- Intruz = włamywacz komputerowy lub inaczej kraker lub inaczej "etyczny haker" czyli kanalia na etacie rządowym. Osoba ta włamuje się zarówno przez sieć, jak też gdy ma fizyczny dostęp do komputera;
- prog. = program;
- bibl. = biblioteka;
- prog. gł. = program główny = jądro = w j. ang. kernel.
- Linuks = Ubuntu, Debian (ale nie Redhat, Fedora, Suse, Gento, Arch);
- sys. = system;
- sys. op. = tak jak j.w. Linuks;
- sys. komp. = system komputerowy, komputer lub sterownik mikroprocesorowy;
- el. = elektronika, elektroniczny;
- pam. = pamięć;
- proc. = procesor;
- konsola = emulator terminala Konsole lub Terminal lub XTerm;
- $USER = twój login w sys. Linuks;
- $HOME = twój katalog domowy w sys. Linuks. Czyli /home/$USER;
- $TWOJE_IP = twoje IP: takie jakie sobie wymyślisz i takie jakie zwraca polecenie ip a po poprawnej konfiguracji sieci;
- edytor = edytor tekstu Nano;
- konf. = konfiguracja;
- wiad. el. = wiadomość elektroniczna.

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, Debian, 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 dwumlask[4]);
- 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 edytor tekstu. Nano jest chyba dostępny we wszystkich dystrybucjach. A na pewno jest dostępny w Debianie i Ubuntu.

4 W j. ang.: double click

- 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

Oficjalna dok. edytora GNU Nano dostępna jest pod adresem https://nano-editor.org/dist/latest/nano.pdf (dostęp w d. 2024-09-16, pon.).

1 Mechanizmy bezpieczeństwa w sys. Linuks

W sys. 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 przedefiniowanie konf. sieci (łącznie z adresami IP i MAC).

Jednak kontrola ruchu sieciowego jest ustalana na poziomie sys. op. (a nie piaskownicy w której działa dany prog.).

4. Zapora sieciowa UFW: Umożliwia globalną kontrolę w sys. op. (niezależnie od firejail) 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. 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. Linuks.

Napędy pojawiają się w sys. jako pliki w kat. /dev natomiast dostęp do ich zawartości uzyskuję dopiero gdy je zamontuję 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 zabolał, to brak rozróżniania 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. 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 montownia dla określonych partycji na urządzeniach podłączanych do komp. z sys. 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. kopi 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. Linuks

Główny podział użytkowników w sys. 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. 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 sieciowych[5].

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 systemowyuch plików konfiguracyjnych.

1.3 Sys. uprawnień w sys. Linuks

Sys. 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:

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

- 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)

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 flagę 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 plikówl, dodawać i usuwać pliki oraz odczytywać ich metadane: rwx;
- Grupa może pobierać listę plikówl oraz odczytywać ich metadane: r-x;
- Pozostali może pobierać listę plikówl oraz odczytywać ich metadane: r-x;

Te domyślne prawa dosępu 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. Linuks).[6]

Dlatego domyślne prawa należy zaostrzyć. 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. Linuks powoduje, że prog. uruchomiony przez użytkownika ma pełen dostęp do jego katalogu domowego. Nie trzeba być wielkim fatalistą by wyobrazić sobie wysyłanie listy moich prywatnych plików na nieznane serwery gdzieś na Świecie. Jasne jest, że to samo może się stać z zawartością co ciekawszych z pośród 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

AppArmor pozwala zaostrzyć prawa dostępu dla konkretnych prog. Można dokładnie określić do jakich konkretnie katalogów i plików prog. ma dostęp.

Prawa dostępu określa dla każdej aplikacji specjalny plik profilu AppArmor. Dostępne są takie pliki z profilami dla popularnych 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.

1.4.2Snap

Snap jest to sys. pakietów firmy Canonical[7] z prog. dla sys. Linuks. Sys. obejmuje też dystrybucję paczek Snap w sieci Internet. Oficjalnie paczki Snap powstały by wprowadzić w sys. Linuks zunifikowany format paczek - wspólny dla wielu dystrybucji. Wymaga to dodawania do paczki części bibl. z jakich ona korzysta. Dodatkowo wmawia się ludziom, że paczki Snap są bezpieczniejsze, bo aplikacje działają w piaskownicy.

Wewnętrznie piaskownice Snap są oparte na profilach AppArmor.

Dużą wadą paczek Snap jest fakt, że użytkownik nie wie do czego prog. ma dostęp. Wynika to z faktu, że jego manifest jest tajny.

Dlatego należy założyć, że paczki Snap żądają pełnego dostępu do kat. domowego.

W POWAŻNYCH ZASTOSOWANIACH JEST TO NIE DO PRZYJĘCIA!!!

Z paczkami Flatpack[8] jest prawdopodobnie tak samo.

DLATEGO SAM NIE UŻYWAM I NIE ZALECAM UŻYCIA PACZEK SNAP ANI FLATPACK.

Poza tym sys. paczek Snap ma wielką wadę: jest b. wolny gdyż zakodowano go w j. skryptowym Pyton.

W sys. Debian możesz sys. Snap zainstalować poleceniem:

```
sudo apt install snapd
sudo snap refresh
```

W Sys. Ubuntu i pochodnych Snap jest zainstalowany domyślnie.

1.4.3AppImage

To popularne paczki z prog. które nie wymagają instalacji i działają w trybie: 1 paczka to 1 aplikacja. By uruchamiać je w piaskownicy należy używać profili firejail z przełącznikiem --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.

1.4.4Ogniste Więzienie czyli Firejail

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

Ogniste Więzienie nie zadziała z prog. instalowanymi z paczek Snap ani z paczkami Flatpack.

Ogniste Więzienie działa w oparciu o AppArmor lub SELinuks. Ma własny format plików z profilami jakie definiują ograniczenia uruchamianych prog.

Ogniste Więzienie wymaga konfiguracji sys. Linuks oraz konfiguracji katalogu użytkownika.

Konfiguracja sys. polega na utworzeniu linków symbolicznych w kat. /usr/local/bin z nazwami prog. jakie maja 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 cudzysłowów).

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.

W sys. Debian pojawia się problem starych profili firejail. Dlatego 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

7 Wydawcy całej rodziny dystrybucji **Ubuntu**.

8 **Flatpack** to konkurencyjny format paczek od firmy **RedHat**.

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.

1.5 Zapory sieciowe

Do kontroli ruchu sieciowego używa się specjalnego prog. ograniczającego ruch sieciowy: zapory sieciowej[9]. 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 w 2024r.: Szwajcaria, Ks. Liechtenstein, Andorra, Irlandia, Meksyk, Monako, San Marino[10][11].

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).

9 W j. ang. firewall

10 Nie można uznać nast. krajów za neutralne: Szwecja (aktualnie w NATO), Miasto Watykan (zawzięte i bezwzględne pedofile), Japonia (aktualnie pod okupacją SZAP).

11 Państw na Ziemi jest 195 (w 2024r.), tak więc jedynie nieco ponad 3,5% z nich jest neutralne. Podczas gdy normalnie powinny być neutralne prawie wszystkie.

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, można jedynie płacić datki. Ta usługa wypełnia def. gratisu (podobnie jak darmowe dystrybucje Linuksa) i to jest nienormalne i dlatego jest to podejrzane.

Cytat z mojej „Ideologii Geniuszy-Mocarzy":„Definicja gratisu jest prosta:

1. Gratis nie podlega reklamacji;
2. Gratis nie gwarantuje niczego. W szczególności nie gwarantuje bezpieczeństwa, ani prywatności, ani przydatności do czegokolwiek;
3. Gratis może ulec zmianie w każdej chwili bez uprzedzenia. W szczególności gratis może ulec degradacji uniemożliwiającej jego dalsze użycie."

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

2 Budowa sieci Internet

Cała sieć Internet (czyli ziemska komputerowa sieć globalna) działa dzięki kom. z sys. rodziny Uniks (w tym sys. Linuks).

Internet został stworzony jako sieć dla sys. op. Uniks 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*1024*1024*1024.

Sieć IPv6 wykorzystuje liczby 128 bitowe do numerowania urządzeń sieciowych. Czyli może być ich 4G*4G*4G*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 IP[12]

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 UDP[13]

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.

12 W j. ang.: Internet Protocol

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

2.2.3 Protokół TCP[14]

TCP jest przesyłany paczkami IP. TCP jest protokołem połączeniowym. TCP dodaje informacje o numerze portu. TCP gwarantuje prawidłową kolejność pakietów i ich poprawność[15].

Najbardziej widocznym zastosowaniem protokołu TCP jest protokół HTTP(S) do przesyłania plików HTML oraz plików pomocniczych[16].

2.3 Sieć lokalna

Sieć lokalną fizycznie tworzy router z portami LAN (kable) i antenami WLAN (fale radiowe). Sieć ta wykorzystuje specjalnie zarezerwowane adresy IPv4[17] lub/i IPv6:

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

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 IP[18] 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.

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

15 W razie potrzeby ponawia transmisję uszkodzonego lub utraconego pakietu.

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

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

18 I to na tej samej karcie sieciowej.

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. Linuks. On jest pośrednikiem który „udaje", że to on wysyła zapytania do serwerów jakie wywołuję, 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 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.

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

Znacznie lepiej samemu ponadawać adresy IP swoim urządzeniom w sieci, gdyż w takim przypadku mogę 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 cyklami[19]. 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. sprytne 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 głupota[20].

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

20 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 podane, że to usługa satelitarna.

3 Ideologia używania sys. Linuks w sieci Internet

3.1 Urządzenia sieciowe: skompromitowane i potencjalnie bezpieczne

Urządzenia kupione, takie jak routery, sprytne TV, sprytne tel., tablety itp. należy uznać za łatwy łup dla każdego intruza.

Należy też uznać, że te wszystkie „sprytne" urządzania pracujące w mojej lokalnej sieci Wi-Fi szpiegują i wysyłają wszystko co się da w Świat. Wynika to po prostu z faktu zerowej możliwości ich konfiguracji.

Urządzenia sieciowe bez możliwości konf. sieci należy uznać za skompromitowane i pod obcą kontrolą.

Sys. samodzielnie zainstalowane, samodzielnie skonfigurowane można nazwać sys. POTENCJALNIE bezpiecznymi.

W zasadzie każda „odchyłka" od normalności w prog. działających w sys. komp. podłączonych do sieci oznacza obecność intruza (etycznego krakera z tajnej policji).

3.2 Fakty o Sys. Linuks

1. Sys. Linuks rodziny Ubuntu to są gratisy. Cytat z mojej monografi "Ideologia Geniuszy-Mocarzy":

„Dzieła kultury na kredyt: Ktoś zaciąga ogromne kredyty by dawać ludziom darmowe dzieła kultury. Youtube Premium za 25,99zł (w mar. 2024r.), to też chyba za półdarmo, bo nawet internet w sprytnym tel. więcej kosztuje.

Definicja gratisu jest prosta:

1. Gratis nie podlega reklamacji;
2. Gratis nie gwarantuje niczego. W szczególności nie gwarantuje bezpieczeństwa, ani prywatności, ani przydatności do czegokolwiek;
3. Gratis może ulec zmianie w każdej chwili bez uprzedzenia. W szczególności gratis może ulec degradacji uniemożliwiającej jego dalsze użycie.

Dzięki p. 1-3 rządy uzyskują kontrolę w dziedzinie kultury i oprogramowania."

To że nie używam komercyjnego sys. Linuks wynika wyłącznie z faktu, że nie ma normalnej, komercyjnej, polskiej dystrybucji sys. Linuks.

2. Domyślnie wszyscy użytkownicy sys. Linuks mają pełen wgląd w katalogi wszystkich innych użytkowników. Łącznie z możliwością kopiowania dowolnych plików oraz z możliwością przeglądania metadanych wszystkich plików - np.: data utworzenia i data ostatniej modyfikacji i wielkość pliku;
3. Sys. op. Linuks gromadzą dane o działaniach użytkownika. Najczęściej w formie plików tekstowych. Często nawet w plikach konf.[21]. Usuwanie tego nie powoduje żadnych zauważalnych efektów;

Z nieznanych powodów w wielu plikach z kat. $HOME/.config i $HOME/.local prog. w sys. Linuks umieszczają unikalne identyfikatory UID. Tak jakby ktoś chciał wiedzieć jakie dokładnie funkcje i czynnności są wykonywane przez użytkowników.

4. Nie wiadomo po co są w sys. Linuks dziesiątki plików cache. Usuwanie tego nie powoduje żadnych zauważalnych efektów.
5. Nie wiadomo po co do sys. Linuks pakuje się masę starych plików: prastarzy użytkownicy sys., prastare grupy użytkowników, kalendarze z przed dziesiątek lat ze świętami z całego świata[22], Usuwanie tego nie powoduje żadnych zauważalnych efektów.

Po usunięciu zbędnych użytkowników i ich grup, są one przywracane "w magiczny sposób" po restarcie

21 np. VLC albo Krusader
22 np. w polskim pliku kalendarza ze świętami jest święto 22 lipca.

komp. CZEMU JEST TO WAŻNE I KOMU NA TYM ZALEŻY???

6. Sys. op. Linuks domyślnie w bramie sieciowej niema włączonych blokad na ruch przychodzący ani wychodzący;

7. W sieci Internet[23] agenci wpływu wmawiają, że problem prywatności dotyczy jedynie społecznościowych serwerów WWW. Podczas gdy:

Domyślnie prog. uruchamiane przez użytkownika mają pełen dostęp do jego katalogu domowego i mogą te dane wysyłać gdzie im się podoba;

8. Poradniki w sieci Internet pokazują jak włączyć bramę sieciową blokującą ruch przychodzący. Ale zupełnie ignorują problem wysyłania w świat danych użytkownika przez prog. szpiegujące na jego komp.;

9. Dane użytkownika wysyłają w świat nawet strony internetowe[24]. Nawet piaskownica przed tym nie chroni. Eksperymenty z prog. ulimit pokazują że najprawdopodobniej dzieje się to przez atak typu przepełnienie bufora przez skrypt z Jawa Skrypt pobierany przez strony HTML.

10. Zapotrzebowanie na pamięć sys. Linuks jest niemożliwe do uzasadnienia: przykład sys. Amiga.

3.3 Ideologia wynikająca z faktów

MOIM GŁÓWNYM CELEM W WALCE Z SYS. LINUKS I Z POWŁOKĄ BASZ JEST ZAPEWNIENIE SOBIE SPOKOJU W PRACY Z KOMP.

DRUGIM CELEM JEST SWOBODNE ROZSZERZANIE MOJEGO ŚWIATOPOGLĄDU, WIEDZY I UMIEJĘTNOŚCI W CELU NOWYCH, REWELACYJNYCH DOKONAŃ.

23 np. na grupie dyskusyjnej pl.comp.os.linux .

24 Miałem przypadek gdy dodałem do czytnika Akregator adres pliku RSS radzieckiej agencji tass.com . Wtedy wystarczyło jedno-jedyne wejście na adres artykułu tej agencji przez przeglądarkę Ognisty Lis (i to uruchomionej w piaskownicy Ogniste Więzienie) i jeszcze tego samego dnia miałem email z zaproszeniem na "randkę z ruską diewuszką".

BO CELEM SZPIEGOSTWA SYS. KOMP. JEST NAMIERZANIE I ELIMINACJA AMBITNYCH OSÓB. BO SPECJALNIACY PARANOICZNIE WIERZĄ, ŻE MYŚLENIE LUDZI IM ZAGRAŻA.

TO JEST POWODEM CAŁEJ AWANTURY O BEZPIECZEŃSTWO I KONIECZNOŚCI SKRYTEJ PRACY I KONIECZNOŚCI PROWADZENIA SKRYTEGO ŻYCIA.

3.3.1 Schemat codziennej pracy z sys. Linuks

1. Konf. sys. po instalacji należy przeprowadzić skryptem (by za każdym razem się nie grzebać).

2. Przy starcie sys. (przed logowaniem) powinien uruchamiać się skrypt czyszczący.

3. Używane prog. należy uruchamiać w piaskownicy Ogniste Więzienie (konieczne jest zakodowanie skryptu konf. i profili lokalnych zaostrzających ograniczenia tych prog.). Zapobiega to wysyłaniu w Świat moich plików przez szpiegujące prog..

4. W skrypcie do konf. zapory sieciowej UFW odblokowuję konieczne adresy IP serwerów z jakimi muszę pracować (np. serwer poczty el., serwer grup dyskusyjnych, serwery z repo). Zapobiega to wysyłaniu w Świat moich plików przez szpiegujące prog..

W przypadku serwerów HTTP które nie ujawniają jakich adresów wymagają ich s. WWW do ich przeglądania należy po prostu używać skompromitowanego sprytnego tel.

5. Pod koniec dnia pracy należy wypchnąć skryptem wszystkie zmienione w ciągu dnia repo.

6. Przed wyłączeniem sys. powinien się uruchamiać skrypt czyszczący.

3.3.2 Comiesięczne czynności konserwatorskie w sys. Linuks

1. Co miesiąc należy wykonywać kopię zapasową prywatnych plików.

2. Spr. czy działa skrypt czyszczący, np.:

```
sudo journalctl -u czysc.service
ls -l /var/cache/man; ls -l
/var/lib/man-db
```

3. Spr. czy w moim kat. prywatnym są nowe pliki z sumami UID, md5 i sha (różnych wer.).
4. Spr. konf. UFW.
5. Zaktualizować sys.
6. Spr. czy są w menu zbędne prog. i je usunąć.
7. Spr. działanie piaskownicy Ogniste Więzienie (co widzą prog. które on kontroluje).

Praca z komp. ma za zadanie automatyzację czynności. Dlatego praca z sys. Linuks wymaga umiejętności programowania skryptów w Baszu.

WSZYSTKIE PONIŻSZE SKRYPTY ZAPROGRAMOWAŁEM I ONE DZIAŁAJĄ - więc ta monografia to nie żadne wzięte z sufitu filozofowanie.

Pamiętaj: JA CI SPRZEDAJĘ WIEDZĘ, A NIE SKRYPTY.

W tym dokumencie pokazuję wszystkie polecenia na jakich należy oprzeć te skrypty. Jednak składni powłoki Basz nie uczę. Nie uczę też zasad proceduralnego programowania - bo Basz to skryptowy język proceduralny.

Poniższe skrypty powinny być tajnym skarbem każdego użytkownika sys. Linuks.

PO ZA SKRYPTAMI JAKIE MAJĄ CZYŚCIĆ SYS. WSZYSTKIE SKRYPTY ODPALAM RĘCZNIE I OBSERWUJĘ CZY NAPOTYKAJĄ JAKIEŚ PROBLEMY.

Wynika to z faktu, że w tych gratisowych sys. Linuks na co dzień dzieją się cuda i nie można samemu przewidzieć wszystkich możliwych problemów.

Proponuję zakodować następujące skrypty:

3.3.3Skrypty konfiguracyjne uruchamiane po instalacji sys.

1. Konf. Basza: konfiguracja plików $HOME/.profile , $HOME/.bash_aliases , $HOME/.bashrc ;
2. Tworzenie linków symbolicznych w kat. $HOME/bin do własnych skryptów.
3. Konf. kart sieciowych;
4. Konf. bramy sieciowej UFW;
5. Konf. piaskownicy Ogniste Więzienie[25].

3.3.4Skrypt czyszczący uruchamiany przed zalogowaniem, przed uśpieniem i przed restartem

Skrypt ten ma czyścić:

1. Zbędne katalogi i pliki w sys. Linuks i w kat. $HOME;
2. Naprawiać plik $HOME/.config/user-dirs.dirs;
3. Usuwać zaw. kat. lost+found
4. Występować ze zbędnych grup użytkowników;
5. Usuwać zbędnych użytkowników;
6. Usuwać zbędne grupy użytkowników;
7. Zaostrzać uprawnienia użytkownika;
8. Usuwać identyfikatory UID i sumy kontrolne z plików tekstowych z kat. $HOME;
9. Usuwać pliki cache podręcznika man;
10. Czyścic kat. $HOME/Pobrane .

3.3.5Skrypt aktualizacyjny

Skrypt aktualizacyjny powinien:

1. Zaostrzać uprawnienia użytkowników;
2. Zaostrzać uprawnienia w sys. Linuks.;
3. Usuwać pliki bez właściciela;
4. Usuwać uszkodzone linki symboliczne;
5. Wyłączać konsolę dla nowych użytkowników;
6. apt update;
7. Konf. Ogniste Więzienie;
8. Wyłączać aktualizację rdzenia sys. Linuks;
9. Usuwać niepotrzebne pakiety;
10. Wyłączenie niepotrzebnych demonów;
11. apt upgrade -y;

25 W j. ang.: firejail

12. Instalować pakiety potrzebne wszystkim użytkownikom;
13. Instalować pakiety potrzebne programistom (w razie potrzeby);
14. Usuwać pakiety zainstalowane przez inne pakiety i już niepotrzebne.

3.3.6 Skrypt konf. zaporę sieciową UFW

Jest to najważniejszy skrypt w zestawie skryptów użytkownika sys. Linuks.

Ten skrypt należy tak zaprogramować aby:

1. Domyślnie blokował cały sieciowy ruch przychodzący;
2. Domyślnie blokował cały sieciowy ruch wychodzący;
3. Standardowo odblokowywał podstawowe serwery UDP (np. DNS z Cloudflare) i TCP (np. drukarki i serwery w sieci lokalnej);
4. Odblokowywał profile sieciowe podane w linii komend (repo, google, poczta, praca, zakupy, nowości).

3.3.7 Skrypt konf. Ogniste Więzienie

Ten skrypt należy tak zaprogramować aby:

1. Kopiował do /etc/firejail moje profile dla prog. jakie chcę kontrolować Ognistym Więzieniem;
2. Tworzył kopię /usr/lib/x86_64-linux-gnu/firejail/firecfg.config;
3. Dodawał moje profile do /usr/lib/x86_64-linux-gnu/firejail/firecfg.config;
4. Kopiował moje lokalne profile do kat. $HOME/.config-firejail;
5. Po jego wykonaniu należy wywołać dla każdego użytkownika:

```
sudo -u $USER firecfg –fix.
```

4 Wybór modelu bezpieczeństwa w pracy z sys. Linuks

4.1 Sys. online

Założenia tego sys.:

1. Instalacja na stacji roboczej wybranego distro i pełna konfiguracja zgodna z zaleceniami tego dokumentu;
2. Całkowita blokada w UFW poł. przych. i wych.;
3. Odblokowywanie w UFW grup zaufanych adresów UDP i TCP dla poł. wych. (np.: serwer z lokalnym repo GIT, DNS, poczta, Google, Wikipedia);
4. Używanie piaskownicy Ogniste Więzienie do kontroli prog.: Grzmiący Ptak[26], Ognisty Lis[27], Ryś[28], wget.

Użycie sieci Internet:

5. Do wariackich s. WWW (które wymagają do działania dodatkowych, nieznanych serwerów) należy używać sprytnego tel. Pliki z tych wariackich s. należy przenosić na komp. za pomocą patyków USB.

Problemem jaki pozostaje w przypadku takiego sys. op. jest fakt używania przeglądarki WWW i klienta poczty el. Problemy z nimi są nast.:

1. Brak jakiegokolwiek audytu/weryfikacji tych podst. klientów sieciowych.
2. Czemu przeglądarki i klient poczty mają monstrualne rozmiary? Czy jest w nich szpiegująca SI?
3. Czemu tak często powstają nowe wer. przeglądarki i klienta poczty? Czemu bez końca się przy nich majstruje?

Pójdźmy krok dalej:

26 po ang. Thunder Bird
27 po ang. Fire Fox
28 po ang. Lynx

4.2 Sys. offline ale online na żądanie

Od poprzedniego modelu ten różni się jednym szczegółem: łączenie z siecią Internet odbywa się jedynie na czas sesji. Np. na czas instalacji potrzebnego prog.

Jednak taki model się nie sprawdzi w firmie gdzie często trzeba odbierać i wysyłać pocztę.

4.3 Sys. z lustrzanym repo

Utworzenie własnego, lokalnego repo używanego distro jest fajną opcją, bo dzięki temu można się zabezpieczyć przed psuciem distro w kol. aktualizacjach oraz przed wył. oficjalnego repo. Dla osoby pracującej serwerek taki 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 i z poza Debian) 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 z github.com . 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 chciano zapewnić paczkom na sprytny tel. jaki Canonical chciało opracować) oraz poprawa bezpieczeństwa przez wbudowaną piaskownicę.

   Nie można wykonać lustrzanej kopi 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 Flatpack 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 Probono[29]. 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.

29 Od łac. "Pro bono publico " - po pol.: Dla dobra publicznego (bez zapłaty).

By skopiować wszystkie paczki prawdopodobnie należało by dać stówę appimagehub.com za taką możliwość.

Założenia tego sys.:

1. Masz łącze światłowodowe (tak rurę do sieci Internet). W przeciwnym wypadku możesz się nie doczekać na pobranie kopi 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 bezczynności[30]. Można to zignorować jeśli po pobraniu kopi lustrzanej repo możesz sobie pozwolić na włączanie 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:

4. Instalacja na stacji roboczej Ubuntu Serwer[31] i pełna konfiguracja zgodna z zaleceniami tego dokumentu.

Ubuntu Serwer od lat ma wadę w instalatorze gdyż partycje na dyskach należy zakładać od nowa za każdym razem.

5. Całkowita blokada w UFW poł. przych. i wych.;
6. Odblokowywanie w UFW poł. przych. ze stacji roboczej;
7. Odblokowywanie w UFW niezbędnych adresów UDP i TCP wychodzących (np.: DNS, repo Ubuntu).

Przygotowanie kopi lustrzanej:

8. Skonfiguruj apache2 tak by użytkownik www-data miał kat. z dokumentami na partycji /home/www-data. Jak to zrobisz to:

By uniknąć problemów utwórz jakiś plik w /home/www-data i spróbuj go pobrać wget - jak to zadziała, to przejdź dalej.

9. Skonfiguruj apt-mirror tak by lustrzane repo było zapisywane do kat. /home/www-data;
10. Należy wykonać kopię lustrzaną repo wybranego distro prog. apt-mirror;
11. Pobrać instalkę wybranego distro z Linksem;
12. Repo aktualizować w ostateczności – zgodnie z pow. zaleceniami.

Konfiguracja stacji roboczej:

13. Instalacja na stacji roboczej wybranego distro i pełna konfiguracja zgodna z zaleceniami tego dokumentu;
14. Całkowita blokada w UFW poł. przych. i wych.;
15. Odblokowywanie w UFW grup zaufanych adresów UDP i TCP dla poł. wych. (np.: lokalne lustrzane repo distro, serwer z lokalnym repo GIT, DNS, poczta, Google, Wikipedia);
16. Konfiguracja apt do pracy z repo na lokalnym serwerze;

Użycie sieci Internet:

17. Do wariackich s. WWW (które wymagają do działania dodatkowych, nieznanych serwerów) należy używać sprytnego tel. Pliki z tych wariackich s. należy przenosić na komp. za pomocą patyków USB.

5 Przygotowanie do instalacji sys. Linuks

Aby w ogóle mieć sys. 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:

30 po ang. idle
31 Główną zaletą Ubuntu Serwer jest wparcie dla programowej macierzy Raid.

5.1 Jaką dystrybucję wybrać?

5.1.1 Wybierz dystrybucję pozwalającą na instalację bez dostępu do sieci Internet

Sys. podczas instalacji jest bezbronny.

Podłączanie komp. do sieci podczas instalacji i późniejsze zabezpieczanie nie ma żadnego sensu.

5.1.2 Są dystrybucje bez zamkniętych pakietów - ale czy warto je instalować?

FSF rozróżnia całkowicie wolne dystrybucje od tych co dodają pakiety z zamkniętym oprogramowaniem[32].

Zamknięte oprogramowanie dotyczy nawet samego rdzenia sys. 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 przesiadki z w pełni wolnej i otwartej dystrybucji Triksel na Kubuntu.

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 .

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

5.2 Jak prawidłowo zainstalować sys. 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 instalki dystrybucji przez intruza. To oznacza:

1. Ściągnięcie instalki dystrybucji sys. Linuks (pliku ISO);
2. Ściągnięcie pliku z sumami kontrolnymi (koniecznymi do weryfikacji oryginalności pliku ISO;
3. Odłączenie komp. od sieci;
4. Spr. obrazu ISO;
5. Nagranie obrazu ISO na USB;
6. Spr. poprawności zapisu obrazu ISO na USB.
7. BEZ WŁĄCZANIA SIECI uruchomić komp. z USB w celu instalacji sys. Linuks.

Jak to wszystko zrobić podaję poniżej.

5.3 Pobieranie obrazu instalki sys. Linuks

By pobrać instalkę Ubuntu, np.:

```
wget
https://releases.ubuntu.com/20.04.5/ub
untu-20.04.5-desktop-amd64.iso
```

Oczywiście powinieneś pobrać aktualnie najnowsze wersje twojej ulubionej dystrybucji sys. Linuks (zamiast tej powyższej).

5.3.1 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.

5.3.2 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. LINUKS POWINIENEŚ ZACZĄĆ OD TEGO MIEJSCA.

5.3.3 Spr. pobranego obrazu

Po pobraniu obrazu należy go spr.:

Ubuntu oferuje na swojej stronie gotowe polecenie. np.:

```
echo
"b45165ed3cd437b9ffad02a2aad22a4ddc691
62470e2622982889ce5826f6e3d *ubuntu-
20.04.1-desktop-amd64.iso" | shasum -a
256 --check
```

Można też to zrobić "normalnie":

```
sha256sum ubuntu-20.04.1-desktop-
amd64.iso
```

I porównać wzrokowo wynik z zawartością pliku z sumami kontrolnymi od dostawcy distro.

5.3.4 Nagrywanie obrazu

Obraz z sys. należy nagrać na pamięć USB. Musi ona mieć co najmniej 4GB.

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. Linuks. Natomiast nikt nie wie co siedzi w 100MB paczce Etcher. Dlatego dla świętego spokoju lepiej użyć dd. Natomiast jeśli używasz Windows to raczej lepszego rozwiązania niż Etcher nie znajdziesz...

5.3.4.1 Rozpoznawanie napędów w sys. Linuks

W sys. Linuks początkujący mogą czuć się zakłopotani jak rozpoznać to gdzie jest podpięta ich pamięć USB (na którą trzeba nagrać obraz ISO z instalką).

W sys. Linuks standardowo dyski 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 .

5.3.4.2 Zapis obrazu na pamięć USB

JAK POMYLISZ NAPĘD SSD Z USB TO MOŻESZ SOBIE WYMAZAĆ DYSK ZE STARYM SYS. OP. TAK WIĘC SPR. 3x CZY ZAPISUJESZ OBRAZ NA PAMIĘĆ USB.

```
dd if=./ubuntu-20.04.1-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.

5.3.4.3 Spr. poprawności zapisu na pamięć USB

Robimy to nietypowym wywołaniem polecenia shasum:

```
sudo shasum -a 256 /dev/sda1
```

Tu są ważne 2 sprawy:

1. Ścieżka do nowo utworzonej partycji na pamięci USB.
2. Algorytm użyty do wygenerowania sumy kontrolnej. Tu sha w wersji 256.

To kiedyś działało, ale obecnie (wrz. 2022) wydawcy dystrybucji robią więcej partycji w instalkach i ja osobiście nie znam sposobu by uzyskać z nich sumę kontrolną taką jaka powstaje przy spr. pliku ISO.

5.4 Uruchomienie instalki

Instalację należy rozpocząć w trybie próbnego uruchomienia sys. Linuks[33]. W tym trybie musimy przygotować się do instalacji przygotowując partycje i przygotowując silne hasło.

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

Proponuję przygotować następujące partycje:

Punkt montowania	Rozmiar	Typ	Przeznaczenie
Bios Grub	1MB	[BRAK][34]	Prog. rozruchowy Grub. Wymagana do uruchomienia sys. z dyskami GPT na starych komp. z BIOS.
/efi	300MB	Fat32[35]	Firmware i prog. rozruchowy. Wymagana do uruchomienia sys. na nowych komp. z UEFI jaki jest następcą BIOS.
/boot	2GB[36]	Ext2	Pliki z obrazami rdzenia sys. Linuks Wymagana do uruchomienia startych komp. z dużymi dyskami. Zabezpiecza przed zapełnieniem dysku przez zbyt dużo starych rdzeni sys. Linuks.
/tmp	20GB[37]	Ext2	Pliki tymczasowe (domyślnie do 10 dni). Zabezpiecza przed zapełnieniem dysku przez zbyt duże pliki tymczasowe.

33 W j. ang.: live mode

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

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

36 Niektórzy zalecają wielkość partycji /boot na 100-300MB. Jednak to się nie sprawdza bo pliki rdzenia sys. **Linuks** mają prawie po 100MB (2021-02). Wydawcy dystrybucji sys. **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 nieznanych powodów zostawiają wiele starych wersji rdzenia. Stąd konieczne zabezpieczenie przed rozrostem katalogu /boot .

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

/var	20GB	Ext2	Pliki różne: w tym kat. /var/tmp (domyślnie do 30 dni), /var/log, /var/cache . Zabezpiecza przed zapełnieniem 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 zapełnieniem dysku przez zbyt duże pakiety nieznanych firm.
/usr/local	20GB	Ext2	Bibl. i prog. samodzielnie budowane i instalowane poleceniami: `rm -fr ./budowa; mkdir ./budowa; cd ./budowa && cmake .. && make -j9; cd .. cd ./budowa && sudo make install && cd ..` Zabezpiecza przed zapełnieniem dysku przez zbyt duże prog. i bibl. instalowane przez użytkownika.
/	100GB	Ext2	Prog. i ustawienia sys. op.
/home	(reszta)	Ext4	Katalogi użytkowników.

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

1. EXT2 nie obsługuje transakcji przy zapisie danych[38];
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. 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. 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.

UWAGA z d. 2022-12-23: Po zainstalowaniu sys. i ustawieniu partycji /tmp i /var z blokadą uruchamiania prog. okazało się, że niemożna aktualizować ani instalować pakietów.

5.6 Pamięć wymiany[39]

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 pamięciożernych procesów.

W sys. 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.

38 W j. ang.: journaling

39 W j. ang.: swap

Partycja swap może szybko zabić dysk SSD, NVM i patyk 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. Obecnie pamięć RAM jest b. tania w porównaniu do lat 90. XXw.

5.7 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 tajnej policji).

Są w sys. 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
```

W śród 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
octyangyitDa
RyclacpesIl5
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}oO
Z.Om\#f<|JSJ
lWw*r}_Y9Ir5
w%:-PgrR=OQs
ng,uD{OOjb<N
LXpzqE+=!>$_
```

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

5.7.1cracklib-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 powłoki[40].

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
```

5.7.2John the Ripper

Po instalacji i konfiguracji sys. Linuks możesz od czasu do czasu sprawdzić siłę haseł użytkowników w sys. prog. John the Ripper. Ten łamacz haseł działa na

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

plikach z sumami obliczonymi z haseł (w przeciwieństwie do cracklib-check który działał bezpośrednio na hasłach).

Oto polecenia instalujące tego łamacza 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 łamacza:

```
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.

5.7.3Zmiana 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.

6 Instalacja sys. Linuks

6.1 Nie łącz się z siecią lokalną ani z Internet

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

6.2 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.

6.3 Wprowadź hasło jakie wygenerowałeś

7 Konfiguracja po instalacji sys. Linuks

7.1 Skonfiguruj sudo

7.1.1Dodaj siebie do grupy sudo

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

```
su -
usermod -aG sudo $USER
```

Wynik możesz sprawdzić poleceniem:

```
id $USER
```

7.1.2 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 UŻYTKOWNIK sudo
```

7.1.3 Włącz sobie użycie sudo bez hasła

Zrób kopię pliku /etc/sudoers:

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

Dodaj linię:

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

Tylko zamiast $USER podaj swój login.

7.2 Skonfiguruj zaporę sieciową UFW

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

Ruch sieciowy mogę obserwować dzięki prog. netstat, tcpdump i Rekin z Drutu[41].

By się dowiedzieć gdzie prog. usiłuje się łączyć, można użyć strace[42].

7.2.1 Domyślne blokowanie całego ruchu sieciowego

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
sudo ufw default reject outgoing
```

Różnica między deny i reject polega na tym, że deny nie odpowiada, natomiast reject odrzuca połączenia. Oznacza to, że reject zachowuje się kulturalnie, ale zdradza obecność kompa w sieci.

Dodatkowo domyślne odrzucanie poł. wych. ma tą zaletę, że nie trzeba czekać na limit czasowy związany z trasowaniem pakietów i rozwiązywaniem nazw przez DNS - oznacza to, że prog. którego blokujemy od razu wznawia normalne działanie, bez oczekiwania na coś co i tak nie nastąpi.

Odblokowuję możliwość łączenia z serwerem w mojej sieci przez ssh:

Na stacji roboczej:

```
sudo ufw allow out from "$TWOJE_IP" to
to 192.168.XXX.XXX port 22 proto tcp
```

Gdzie 192.168.XXX.XXX to adres serwera w sieci lokalnej.

Na serwerze:

```
sudo ufw allow in from "$TWOJE_IP" to
to 192.168.XXX.XXX port 22 proto tcp
```

Zamiast allow można użyć limit zabezpiecza to przed atakiem odmowy dostępu[43] (czyli przed zbyt dużą ilością jednoczesnych połączeń przychodzących). Jednak problemem wtedy są skrypty które używają SSH (np. skrypt do wypychania wszystkich repo git na koniec dnia).

7.2.2 Odblokowanie możliwości łączenia się z serwerami DNS

Trochę pomęczyłem google.pl i duckduckgo.com w sprawie zalecanych serwerów DNS. Mi chodziło, czy są jakieś "wolne" serwery DNS lub chociaż zalecane przez EFF lub GNU, ale nic takiego nie znalazłem. Dlatego

41 W j. ang.: wireshark

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

43 W j. ang.: access denied

wybrałem po prostu najszybsze serwery DNS od Cloudflare z Kaliforni w SZAP.

Serwery DNS nasłuchują na porcie 53.

Wynikowe polecenia odblokowujące serwery DNS od Cloudflare są takie:

```
sudo ufw allow out from "$TWOJE_IP" to
1.1.1.1 port 53 proto udp
sudo ufw allow out from "$TWOJE_IP" to
1.0.0.1 port 53 proto udp
```

7.2.3 Odblokowanie synchronizacji zegara z serwerem czasu NPT

Aby się nie rozdrabniać serwer czasu też wybrałem Cloudflare. Aby używać tych serwerów należy wyedytować plik:

```
sudo nano /etc/sys.d/timesyncd.conf
```

I zmienić w nim linię:

```
#NTP=
```

Na:

```
NTP=time.cloudflare.com
```

Następnie należy zrestartować demona synchronizacji zegara:

```
sudo systemctl restart sys.d-
timesyncd.service
```

Następnie należy odblokować w UFW możliwość łączenia z serwerem time.cloudflare.com, dlatego najpierw należy spr. jaki jest jego adres IP.

Aby ustalić adresy IP nazw domenowych używam prog. dig.

```
$ dig time.cloudflare.com
time.cloudflare.com.    31      IN
A       162.159.200.1
time.cloudflare.com.    31      IN
A       162.159.200.123
```

Serwery NPT nasłuchują na porcie 123.

Wynikowe polecenia odblokowujące serwery NPT od Cloudflare są takie:

```
sudo ufw allow out from "$TWOJE_IP" to
162.159.200.1 port 123 proto udp
sudo ufw allow out from "$TWOJE_IP" to
162.159.200.123 port 123 proto udp
```

Dokończenie konfiguracji ufw będzie omówione po połączeniu z Internet.

7.2.4 Odblokowanie możliwości łączenia z repo Ubuntu

```
dig archive.ubuntu.com
[...]
archive.ubuntu.com.     54      IN
A       91.189.91.39
archive.ubuntu.com.     54      IN
A       185.125.190.36
archive.ubuntu.com.     54      IN
A       185.125.190.39
archive.ubuntu.com.     54      IN
A       91.189.91.38
[...]

dig security.ubuntu.com
[...]
security.ubuntu.com.    24      IN
A       91.189.91.38
security.ubuntu.com.    24      IN
A       91.189.91.39
security.ubuntu.com.    24      IN
A       185.125.190.36
security.ubuntu.com.    24      IN
A       185.125.190.39
[...]
```

Jak widać oba adresy mają takie same numery IP (jedynie w innej kolejności). Ja osobiście tego nie rozumiem, ale widać takie szaleństwa też są możliwe.

Wynikowe polecenia odblokowujące te adresy na portach http, czyli 80 i https czyli 443 są takie:

```
sudo ufw allow out from "$TWOJE_IP" to
91.189.91.39 port 80 proto tcp
sudo ufw allow out from "$TWOJE_IP" to
185.125.190.36 port 80 proto tcp
sudo ufw allow out from "$TWOJE_IP" to
185.125.190.39 port 80 proto tcp
sudo ufw allow out from "$TWOJE_IP" to
91.189.91.38 port 80 proto tcp
sudo ufw allow out from "$TWOJE_IP" to
91.189.91.39 port 443 proto tcp
sudo ufw allow out from "$TWOJE_IP" to
185.125.190.36 port 443 proto tcp
sudo ufw allow out from "$TWOJE_IP" to
185.125.190.39 port 443 proto tcp
```

```
sudo ufw allow out from "$TWOJE_IP" to
91.189.91.38 port 443 proto tcp
```

7.2.5 Odblokowanie możliwości łączenia z serwerami Google

Tego nie da się zrobić ręcznie. Do skryptu konf. UFW należy dodać kod który:

1. Odblokowuje w UFW adresu IP do jakiego kieruje domena www.gstatic.com;
2. Pobiera listę zakresów IP serwerów Google:

https://www.gstatic.com/ipranges/goog.json
https://www.gstatic.com/ipranges/cloud.json

3. Wyciąga wszystkie zakresy IP z pow plików;
4. Odblokowuje zakresy adresów Google w UFW;
5. Usuwa pliki goog.json i cloud.json.

7.2.6 Odblokowanie możliwości łączenia z serwerem duckduckgo.com

```
dig duckduckgo.com
[...]
duckduckgo.com.         125     IN
A       40.114.177.156
[...]
```

Wynikowe polecenie odblokowujące ten adres jest takie:

```
sudo ufw allow out from "$TWOJE_IP" to
40.114.177.156 proto tcp
```

7.3 Konfiguracja prog. gł. sys. Linuks

Aby dostroić sam prog. gł. sys. 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:
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_respo
nses= 1
```

Następnie wydaj polecenie:

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

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

```
sudo sysctl --system
```

7.4 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,n
odiratime,noiversion,norelatime,
nostrictatime,lazytime,nouser 0
0
```

7.5 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 wyłacza się go edytując plik:

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

Tam trzeba zakomentować (znakiem #) linię:

```
# /swapfile       none            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
```

7.6 Włącz automatyczne ubijanie zbyt żarłocznego procesu

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

Powłoka Basz 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"[44] 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"[45].

W przypadku trybu interaktywnego: cytat: "[...] bash czyta i wykonuje polecenia z /etc/bash.bashrc i ~/.bashrc, jeśli takie pliki istnieją"[46].

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 ustawione. 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.
```

---

44 man bash
45 tamże
46 tamże

Należy dodać takie linie:

```
ulimit -v $((80*1024*1024))
```

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

```
ulimit -m $((20*1024*1024))
```

To jest limit rzeczywistego użycia pamięci przez proces użytkownika.

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"[48].

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

```
ulimit -u 1024
```

7.7 Zaostrz prawa dostępu do katalogów użytkowników

7.7.1Katalogi 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 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 - LOGIN
```

Gdzie LOGIN 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[49].

7.7.2UMASK

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

Czyli gdy ma ona wartość 077 to 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.

7.7.2.1 UMASK globalny

W pliku

sudo nano /etc/login.defs

ustaw:

```
UMASK 077
USERGROUPS_ENAB no
```

47 Ta dziwna konstrukcja z $(()) to wyrażenie matematyczne w Baszu obliczające ile KB jest w 20GB.

48 Akregator (czytnik RSS) potrafi wykorkować przy niskich wart. limitów pam., podobnie prog. Jawa (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).

49 Pod warunkiem, że w **UFW** zostały odblokowane odpowiednie adresy.

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

7.7.2.2 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 Pytona 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
```

7.7.2.3 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
```

Nalezy dodać linię:

```
umask 077
```

7.7.3DIR_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 edytuję:

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

ustawiam:

```
DIR_MODE=0700
```

Czyli zapewniam wyłącznie sobie odczyt, zapis i wykonanie.

7.7.4Ważne pliki sys.

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

7.8 Usuń pliki bez właściciela

```
sudo find / -xdev \( -nouser -o -
nogroup \) -print0 | xargs -0 -ixxx
sudo rm -r xxx
```

To polecenie może kasować konteneray Dokera.

7.9 Usuń uszkodzone linki symboliczne

Po usunięciu oryginalnego pliku do którego prowadził link symboliczny ten link pozostaje w sys. Jest on wtedy „uszkodzonym linkiem symbolicznym”. Generalnie należy się ich pozbyć:

```
sudo find / -xtype l -delete
```

To polecenie może kasować kontenery Dokera.

7.10 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
```

7.11 Konfiguracja sys. Linuks dla programisty

7.11.1 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 hard[50] i soft[51] 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. Linuks:

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

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

```
sudo sysctl --system
```

50 Jest to nieprzekraczalny limit w sys..

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

7.12 Konfiguracja sys. Linuks dla nie programisty

7.12.1 Wyłącz zrzuty prog. gł. i pozostałych prog.

Wyedytuj:

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

I ustaw:

```
* - core 0
```

7.13 Konfiguracja użytkowników

Razem z sys. Linuks jest instalowana cała masa niepotrzebnych użytkowników. Zalecam dodanie takiej sekwencji poleceń do własnego skryptu aktualizacji sys.:

```
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
```

7.14 Konfiguracja grup 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.icznych). Aby wystąpić z tych grup należy użyć polecenia:

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

Na pewno należy usunąć te grupy z sys.:

```
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
```

7.15 Ogniste Więzienie

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 co prog. może robić a czego mu nie wolno. Do tych prog. zaliczamy Ogniste Więzienie (w j. ang. Friejail). Jest on przykrywką dla AppArmor (Debian/Ubuntu) i SeLinux (RedHat).

Przykładowo gdy uruchomimy Grzmiący Ptak w Ogniste Więzienie, to Grzmiący Ptak będzie miał dostęp tylko do kat. $HOME/Pobrane i paru plików w $HOME. Tak więc nic nie jest w stanie nam ukraść.

Ogniste więzienie nie pozwala na konf. zapory sieciowej dla każdego prog. z osobna.

7.15.1 Instalacja Ogniste Więzienie

```
sudo apt install firejail
```

7.15.2 Włączenie Ogniste Więzienie

Włączenie Ogniste Więzienie jest dwu etapowe:

1. Najpierw trzeba zlinkować ograniczane prog. do /usr/local/bin . Robi się to dlatego, że prog. uruchamiany w skróconej formie jest wyszukiwany najpierw w /usr/local/bin a jak tam go nie ma to szukany jest w /usr/bin .

```
sudo firecfg
```

2. Następnie trzeba usunąć ścieżki /usr/bin ze wszystkich poleceń w plikach *.desktop[52] by uruchamiały one prog. z /usr/local/bin (bo ma on wyższy priorytet nad /usr/bin). Robi to polecenie:

```
firecfg --fix
```

7.15.3 Uruchamianie prog. w piaskownicy Ogniste Więzienie i bez niej

Po tych zabiegach uruchamianie prog. odbywa się wg schematu:

```
/usr/bin/thunderbird     # Grzmiący
Ptak uruchomi się bez piaskownicy
thunderbird              # Grzmiący
Ptak uruchomi się w piaskownicy
```

Czyli podając pełną ścieżkę (tu: /usr/bin/XXXXX) pomija sie Ogniste Więzienie. Natomiast wydając skrótowe polecenie prog. uruchamiany jest w piaskownicy.

7.15.4 Spr. czy prog. jest uruchomiony w piaskownicy Ogniste Więzienie

```
firejail --list
```

7.15.5 Strojenie Ogniste Więzienie

Uprawnienia prog. zdefiniowane w kat. /etc/firejail są bardzo restrykcyjne, a czasem wręcz nieżyciowe. Dla niektórych prog. w ogóle brak profilów Ogniste Więzienie.

To że profile Ogniste Więzienie nie odpowiadają w 100% naszym potrzebom nie znaczy, że Ogniste Więzienie jest zły. Oznacza to, że Ogniste Więzienie

52 Są to pliki opisujące skróty z ikonami na pulpicie.

trzeba dostrajać zamiast się niepotrzebnie denerwować.

Ogniste Więzienie dostrajamy tworząc pliki $HOME/.config/firejail/*.local . Pliki te mają taką samą składnię jak pliki /etc/firejail/*.profile .

Tu podam kilka przykładów jak dostrajam Ogniste Więzienie:

1. Kate - edytor tekstów - powinien nie mieć dostępu do sieci Internet i powinien mieć dostęp do wszystkich plików w kat. domowym. Dlatego w pliku $HOME/.config/firejail/kate.local mam taki wpis:

```
net none

noblacklist ${HOME}
read-write ${HOME}

blacklist /opt
```

Tak samo mam skonfigurowanego Qt Creatora - IDE do prog. w C++.

2. Libreoffice - pakiet biurowy - nie powinien mieć dostępu do sieci Internet i powinien mieć dostęp do kat. Dokumenty, Ściągnięte i Szablony, wiec w pliku $HOME/.config/firejail/libreoffice.local mam taki wpis:

```
net none

whitelist ${HOME}/Dokumenty
whitelist ${HOME}/Ściągnięte
whitelist ${HOME}/Szablony

blacklist /opt
```

3. Ognisty Lis - przeglądarka stron www - powinien mieć dostęp do kat. $HOME/Ściągnięte więc w pliku $HOME/.config/firejail/firefox.local mam taki wpis:

```
whitelist ${HOME}/Ściągnięte

blacklist /opt
```

4. Grzmiący Ptak - powinien mieć dostęp do kat. $HOME/Ściągnięte i do kat. $HOME/.gnupg, a dodatkowo w tym profilu musi działać Google Chrome, więc w pliku $HOME/.config/firejail/thunderbird.local mam taki wpis:

```
whitelist ${HOME}/+Ściągnięte

ignore noexec /tmp
ignore noexec ${HOME}
ignore caps.drop all
ignore ipc-namespace
ignore no3d
ignore nonewprivs
ignore noroot
ignore novideo
ignore protocol
ignore seccomp
ignore private-bin
ignore private-etc
ignore private-tmp
ignore dbus-user none
ignore dbus-system none
ignore memory-deny-write-execute

noblacklist
${HOME}/.cache/BraveSoftware
noblacklist
${HOME}/.config/BraveSoftware
noblacklist ${HOME}/.config/brave
noblacklist ${HOME}/.config/brave-
flags.conf
noblacklist ${HOME}/.gnupg
noblacklist /proc/config.gz
noblacklist ${HOME}/.pki
noblacklist ${HOME}/.local/share/pki

mkdir ${HOME}/.cache/BraveSoftware
mkdir ${HOME}/.config/BraveSoftware
mkdir ${HOME}/.config/brave
whitelist ${HOME}/.cache/BraveSoftware
whitelist
${HOME}/.config/BraveSoftware
whitelist ${HOME}/.config/brave
whitelist ${HOME}/.config/brave-
flags.conf
whitelist ${HOME}/.gnupg

caps.keep sys_admin,sys_chroot

whitelist /opt/google
```

7.15.6 Dodawanie brakujących profili Ogniste Więzienie

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 Ogniste Więzienie:

Do pliku /usr/lib/x86_64-linux-gnu/firejail/firecfg.config należy dodać wpis "nazwa_programu" (bez cudzysłowu).

Zwróć uwagę, że ten plik jest posortowany. Więc by uniknąć problemów należy dodać nazwę prog. we właściwym miejscu w tym pliku (programując skrypt należy zrobić kopię zapasową firecfg.config następnie na jego koniec dodać nazwa_progarmu i przepuścić przez rurkę sort|uniq).

4. Ponowna konfiguracja Ogniste Więzienie:

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

7.15.7 Globalne wyłączenie Ogniste Więzienie

Normalnie nie jest potrzebne wyłączanie Ogniste Więzienie.

By go ominąć wystarczy podać pełną ścieżkę do prog. np.:

```
/usr/bin/thunderbird    # Grzmiący
Ptak uruchomi się bez piaskownicy
thunderbird             # Grzmiący
Ptak uruchomi się w piaskownicy
```

Jednak gdy chcesz koniecznie wyłączyć Ogniste Więzienie, to znam dwie metody:

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

albo:

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

7.16 SSH

7.16.1 Instalacja ssh

Tam podano niektóre czynności dotyczące serwerów i klientów linuksowych.

Na stacji roboczej instaluję klienta ssh poleceniem:

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

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.

7.16.2 Konfiguracja 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:

```
# Wymuszenie protokołu w wersji 2:
Protocol 2
# Blokada logowania roota:
PermitRootLogin no
# Blokada pustych haseł:
PermitEmptyPasswords no
# Wymuszenie uwierzytelniania za
pomocą klucza publicznego:
PasswordAuthentication no
ChallengeResponseAuthentication no
UsePAM no
# Blokada identyfikacji po nazwie
komp.:
IgnoreRhosts yes
HostbasedAuthentication no
# Wyłączenie przekierowań ruchu TCP
AllowTCPForwarding no
# Blokada uruchamiania prog. graf.:
X11Forwarding no
# Adres na jakim nasłuchuje sshd
(chodzi o to żeby nie nasłuchiwał na
publicznym IP):
ListenAddress 192.168.20.XXX

# Obsługa użytkowników wyłącznie z
sieci lokalnej:
AllowUsers *@192.168.20.YYY
```

```
# albo dla wszystkich komp. w sieci lokalnej: AllowUsers *@192.168.20.0/24

# Ustawienie kat. chroot w celu ograniczenia dost. do wybranego kat.
Match User git
ChrootDirectory /home/git/projekty
```

XXX zastępuję końcówką adresu IP swojego serwera.

YYY zastępuję końcówką adresu IP swojej stacji roboczej.

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

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

7.16.2.1 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 (tego rozpoznaje SSH w Debian 10):

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

7.16.2.2 Załaduj publiczne klucze SSH na serwer[53]

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.

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
```

7.16.3 Wykonaj instrukcję SSH Hardening Guides

https://www.ssh-audit.com/hardening_guides.html

7.16.4 Użyj ssh-audit by spr. konf. serwera ssh

```
ssh-audit 192.168.20.24
```

7.17 Skonfiguruj CUPS

CUPS to demon drukowania. Udostępnia on zbędną usługę konfiguracji przez stronkę WWW. Jest to zbędne

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

bo to samo można robić z poziomu menadżera okien. Aby to wyłączyć edytujemy plik:

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

Szukam lini:

```
WebInterface Yes
```

I zmieniam na:

```
WebInterface Off
```

Następnie zrestartuj cups:

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

7.18 Skonfiguruj zegary

W sys. Linuks zegary uruchamiają regularnie różne zadania. Część z tych zadań jest nadmiarowa. Do kontroli zadań okresowych służy cron i systemd. Zegary z systemd tak naprawdę powielają to co oferuje cron.

Aby przejrzeć zad. cron, należy spr. zaw. nast. kat.:

```
/etc/cron.hourly
/etc/cron.daily
/etc/cron.weekly
/etc/cron.monthly
```

Z tych kat. należy usunąć (czyli przesunąć do kat. domowego) pliki zadań takich jak:

- Budowanie bazy man-db (jej brak nic widocznego nie powoduje – prawdopodobnie służy celom szpiegowskim);
- Zadania apt (ich brak nic nie powoduje – prawdopodobnie służą celom szpiegowskim).

Zad. zegarowe systemd listuje komenda:

```
sudo systemctl status *.timer
```

Tu podobnie należy usunąć (czyli przesunąć do kat. domowego): man-db.timer, apt-dialy-update.timer i apt-dialy.timer. Znajdują się one w kat.:

```
/usr/lib/systemd/system
```

Świadomie podaję, że należy kasować te pliki, bo standardowa komenda:

```
sudo systemctl disable man-db.timer
```

Po prostu nie działa (zegar jest natychmiast ponownie uruchamiany).

7.19 Skonfiguruj sieć

Pamiętaj $TWOJE_IP to adres twojego kompa 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 twojego sys. 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. 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.

   Najsensowniejszą znaną mi konfiguracją sieci w sys. Linuks w 2023r. jest netplan. Tą konfigurację definiuje się w plikach *.yaml i kopiuje się je do kat. /etc/netplan .

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. Linuks?

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

XXXXXXXX jest nazwą twojej karty sieciowej w sys. Linuks.

5. 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: "XXXXXXXXXXX"
      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.). "XXXXXXXXXXX" 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.

7.20 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:

```
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
```

7.21 Postarzanie prog. gł.

7.21.1 Blokada aktualizacji prog. gł.

Mnie osobiście bardzo dziwi i bardzo niepokoi cotygodniowa aktualizacja prog. gł. w dystrybucjach bazujących na Debianie. Nie wnikam co tam oni mieszają, tylko po instalacji wydaję polecenie:

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

7.21.2 Instalacja najstarszego prog. gł. 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.

7.21.3 Uruchom ponownie sys. komp. wybierając w boot menu starą wer. prog. gł.

7.21.4 Wyłączenie blokad usuwania zbędnych wer. prog. gł.

```
sudo nano
/etc/apt/apt.conf.d/01autoremove
```

I zakomentuj wszystko w sekcji NeverAutoRemove:

```
  NeverAutoRemove
  {
#       "^firmware-linux.*";
#       "^linux-firmware$";
#       "^linux-image-[a-z0-9]*$";
#       "^linux-image-[a-z0-9]*-[a-z0-
9]*$";
  };
```

7.21.5 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 zainstalować 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:

```
/boot/System.map-5.4.0-96-generic
/boot/config-5.4.0-96-generic
```

7.22 Skrypt aktualizujący sys.

Aktualizacja sys., to nie tylko banalne:

```
sudo apt update && sudo apt upgrade
```

Konieczne jest wykonanie dużo większej ilości działań. Dlatego proponuję napisać skrypt w którym dzieją się rzeczy opisane w p. Skrypt aktualizacyjny.

8 Ręczna diagnostyka bezpieczeństwa

8.1 Diagnostyka transmisji w sieci Internet

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

```
sudo tcpdump
```

Jednak gdy chcesz zobaczyć tylko nowe połączenia. By wiedzieć co się dzieje z twoim komp. należy użyć opcji pokazujące tylko pakiety IP/TCP z flagą SYN:

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

Gdy chcesz monitorować tylko rozpoczynanie 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 zabezpieczenie[54][55] by nie mógł działać w skryptach.

Do wyświetlania otwartych gniazd Internet TCP, podawania nazwy procesu (gdy to możliwe), bez obcinania adresu, z dodatkowymi informacjami, ze wszystkimi gniazdami i z powtarzaniem - należy użyć polecenia:

```
sudo netstat -tpWeea --numeric-ports
```

Gdy uruchmisz netstat bez sudo nie zobaczysz nazw prog.!

Gdy chcesz ciągle monitorować otwarte połączenia prog. netstat, użyj opcji --continuous :

```
sudo netstat -tpWeea --numeric-ports --continuous
```

8.2 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.

---

54 Dla dociekliwych: zabezpiecznie w **tcpdump** przed użyciem w skryptach polega na spr. czy plik **STDOUT** to urządzenie kolejką typu FIFO (to **tcpdump** sprawdza w skrypcie) czy znakowe (to tcpdump sprawdza w konsoli). Jak jest znakowe to **tcpdump** drukuje normalne komunikaty, ale jak jest FIFO to **tcpdump** nic nie drukuje. Ja badałem ten problem i wygląda mi na to, że zabezpieczenie to jest gdzieś w bibl. **pcap**. Myślę tak dlatego, że **tcpdump** używa bibl. **pcap** z której dostaje dane przez f. zwrotną (ang.: callback). Ja w tcpdump we wszystkich jego f. zwrotnych dodałem komunikat z nazwą f. i trzema wykrzyknikami. Przy wywołaniu z konsoli wyświetla się komunikat "**print_packet!!!**". Natomiast wywołując **tcpdump** w skrypcie żaden komunikat się nie wyświetla. Dodatkowym problemem jest fakt, że spr. rodzaju pliku **STDOUT** odbywa się f. sys.ową **fstab**, ale nie ma jej wywołania ani w źródłach **tcpdump** ani w źródłach **libpcap**. Jest ona używana jedynie w prog. testujących bibl. **pcap**.

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

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

8.2.1 Test skanowania portów

Po pierwsze należy ustalić adres ip twojego komp.

Na nowo zainstalowanym sys. Linuks wywołaj:

```
ip a
```

Interesuje cię linia w stylu:

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

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

Mogę spr. jakie są otwarte porty na moich sys. w sieci lokalnej. Robi to polecenie:

```
nmap -Pn 192.168.XXX.XXX
```

To skanowanie z opcjami -Pn ma taką wadę, że obejmuje tylko pierwsze 1K portów. Użyłem ich dlatego, że pełne skanowanie, czyli opcja -p-, w ogóle nie wykrywa komp. z zaporą skonfigurowaną w podany w tej monografii sposób.

8.2.2 Test dostępu do otwartego portu zablokowanego przez UFW

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

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

Natomiast na drugim komp. wywołaj polecenie:

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

Gdy jest ok możliwe są 2 rezultaty:

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

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

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

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

8.3 Skaner debsums (spr. sumy kontrolne pakietów)

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.

Ten skaner podaje listę plików jakie uległy zmianie po instalacji. Domyślnie listuje on wszystkie sprawdzane pliki co jest trochę przytłaczające. Wtedy pomaga 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
```

8.4 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.[56]

8.4.1 Instalacja

```
sudo apt install lynis
```

8.4.2 Skanowanie

```
sudo lynis audit system
```

56 https://en.wikipedia.org/wiki/Lynis

8.4.3Interpretacja 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.

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)
[…]
```

8.5 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.).

8.5.1Instalacja

```
sudo apt install rkhunter
```

8.5.2Aktualizacja

```
sudo rkhunter --propupd
```

8.5.3Skanowanie

```
sudo rkhunter --check
```

8.5.4Interpretacja 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:
```

8.6 Skaner Debsecan (poszukuje exploit-ów)

Exploit – prog. mający na celu wykorzystanie istniejących błędów w oprogramowaniu.[57]

8.6.1 Instalacja

```
sudo apt install debsecan
```

8.6.2 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:

```
$ 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)
[…]
```

8.7 Skaner Fail2ban (pokazuje nieudane próby logowania)

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

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

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

8.8 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.

57 https://pl.wikipedia.org/wiki/Exploit

p0f[58]	• 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	• 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).
fragrouter	Przechwytywanie i modyfikacja ruchu w sieci. Prog. wydaje się niepraktyczny gdy HUB LAN (kablowe) wyszły z użycia (zastąpiły je router z wbudowanymi switch LAN (kablowe) i WLAN (radiowe)).
strobe (pakiet netdiag)	Wykrywanie otwartych portów.
irpas	Zestaw programów: • 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 Automatyzacja monitorowania bezpieczeństwa

Kiedyś była wypasiona, francuska dystrybucja sys. 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:

58 Co ciekawe jest to prog. Amerykanina polskiego pochodzenia.

9.1 Skrypt monitorujący nawiązywanie i rozłączanie poł. przychodzących i wychodzących

Skrypt ten jest oparty na tcpdump. Zakodowałem go w Baszu i jestem pewnien jego poprawności (2022-09-10 i 2022-09-11 parę godzin go testowałem). Skrypt ten nie działa gdyż tcpdump blokuje się gdy używa się go w skryptach. Więcej na ten temat było wyżej.

9.2 Skrypt monitorujący odrzucanie poł. przychodzących i wychodzących

Skrypt ten jest oparty na monitorowaniu pliku /var/log/ufw.log prog. tail jaki podaje dane na wejście prog. read w pętli while. Ładnie to działa i wszystko widać jak na dłoni.

9.3 Skrypt monitorujący stan aktywnych połączeń w sieci Internet

Skrypt jest oparty na prog. netstat i wywołuje go co parę sekund. Jego wyjście po przekształceniu jest czytelne ale nie do oglądania w czasie rzeczywistym bo raz, że to atrakcja jak wędkowanie, a dwa ekran miga jak diabli.

10 Skryte korzystanie z sys. Linuks

10.1 Skrypt czyszczący

Należy sobie zaprogramować skrypt czyszczący gdyż nie wiadomo po co w sys. Linuks są gromadzone dane o historii działań użytkownika.

Nie wiadomo też dlaczego w sys. jest mnóstwo plików cache. Usuwanie tych plików nie wprowadza żadnych opóźnień w działaniu sys. ani prog.!!!

Ten skrypt przed niczym nie zabezpiecza, ale daje święty spokój. Czyścić należy:

- Historię poleceń konsoli;
- Historię edytowanych plików;
- Historię odwiedzanych stron WWW;
- Kasować katalogi i pliki tmp, cache i hist;
- Archiwa w katalogach ukrytych w $HOME/.*;
- Zbędne logi;
- Usuwać należy nr UID, sumy MD5 i SHA (wszystkich wer. - począwszy od najdłuższych sha512).

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

Należy też przejrzeć pliki w kat. /var .

W kat. /var należy zostawić w spokoju wszystkie pliki związane z apt i dpkg!!! Ich kasowanie grozi nieodwracalnym uszkodzeniem sys. op. tak, że niczego nie będzie można zainstalować ani odinstalować (mimo, że reszta będzie normalnie działać).

Skrypt czyszczący należy uruchamiać gdy:

- Uruchamia się sys. op. - robi to spec. plik czyszczenie.service:

Przy proponowanym podziale na partycje może się okazać, że partycja $HOME nie jest zamontowana w momencie uruchomienia skryptu czyszczącego. Dlatego należy go kopiować do kat. /usr/bin (i w inne miejsca gdzie jest on potrzebny).

```
[Unit]
Description=czysc.sh
Before=network.target

[Service]
Type=idle
ExecStart=/usr/bin/czysc.sh
Restart=on-failure
RestartSec=120
KillMode=process

[Install]
WantedBy=multi-user.target
```

Należy go zainstalować:

```
systemctl daemon-reload
cp -f "$lKatZrudlowy/czysc.service"
"/etc/systemd/system/"
sed -i -r
's|ExecStart=.*|ExecStart=/usr/bin/czy
sc.sh|g'
"/etc/systemd/system/czysc.service"
systemctl daemon-reload
systemctl enable czysc.service
```

Dodatkowo należy wprowadzić poprawkę do pliku /lib/systemd/system/systemd-networkd.service, tak by czekał on na wykonanie czysc.sh. Polega to na dodaniu czysczenie.service do zmiennej After=:

```
cp /lib/systemd/system/systemd-
networkd.service
/lib/systemd/system/systemd-
networkd.service.org
sed -i -r 's|After=(.*)|After=\1
czysc.service|g'
/lib/systemd/system/systemd-
networkd.service
   systemctl daemon-reload
```

- Gdy zamyka się sys. - wywołując kopię /lib/sys.d/sys.-shutdown/czysc.sh;
- Gdy usypia się sys. - wywołując kopię /lib/sys.d/sys.-sleep/czysc.sh;
- Gdy uruchamia się pulpit (chodzi o przypadek gdy użytkownik się przelogowuje – wtedy sys. też powinien być czyszczony).

10.2 Wyłącz raporty o błędach

```
sudo systemctl stop apport.service
sudo systemctl disable apport.service
sudo systemctl mask apport.service
sudo apt remove --purge -y ubuntu-
report
sudo systemctl stop whoopsie.service
sudo systemctl disable
whoopsie.service
sudo systemctl mask whoopsie.service
sudo apt remove --purge -y whoopsie
```

10.3 Wyłącz raporty popularności pakietów

```
sudo apt remove --purge -y popularity-
contest
```

Aby zablokować użytkownikom dostęp do tej usuniętej usługi edytuję plik:

```
sudo nano /etc/dconf/profile/userfile
```

I dodaję w nim zawartość:

```
user-db:user
system-db:local
```

Następnie wprowadzam zmiany w życie:

```
sudo dconf update
```

10.4 Wyłącz informowanie o obecności w sieci

Dotyczy to chyba wyłącznie starszych wersji Ubuntu (przed 20.04).

Aby to wyłączyć należało wyedytować plik:

```
sudo nano
/var/lib/NetworkManager/NetworkManager
-intern.conf
```

I zmienić w nim flagę:

```
[connectivity]
```

```
set.enabled=false
```

11 Skryte korzystanie z sieci Internet

11.1 Przeszkody w skrytym korzystaniu z Internetu

11.1.1 Przeglądarki mają pełen dostęp do kat. domowych wszystkich użytkowników w sys. Linuks.

W Ubuntu domyślne prawa dostępu do kat. innego użytkownika są ustawione tak by łatwo można mu było wszystko ukraść. Nawet więcej! Domyślnie jest możliwość odczytu kat. domowego wszystkich innych użytkowników.

W tym dok. podaję jak sobie z tym radzić. Oczywiście mówię o zaostrzaniu uprawnień użytkownika i użyciu piaskownicy Ogniste Więzienie. 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 Fire Fox 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. Linuks (j. w.);
3. Inny znany problem dotyczy przeglądarki Water Fox, która ma zabezpieczenia przed pracą w piaskownicy Ogniste Więzienie. 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 uniemożliwić kontrolę użytkownika nad przeglądarkami.

11.1.2 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, Water Fox lub Fire Wolf powinny mieć wtyczkę która powinna pozwalać na pełną edycję danych identyfikacyjnych, oraz ich maskowanie (wart. stałymi lub losowanymi).

Niestety obecnie (2023r.) 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 w.w. 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.

11.1.3 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.

11.1.4 Dostawcy Internetu 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.

11.1.5 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.

11.1.6 Sprawa Amejzon

Takie firmy jak Google czy Amejzon używają dużej l. adresów IP. Może się zdarzyć, że chcemy je odblokować w UFW. Dobre jest to, że obie firmy, jako nieliczne, publikują pliki z listami zakresów używanych przez nie adresów IP. Google się wycwaniło i wcześnie wykupiło zakresy adresów IP wer. 4. Natomiast Amejzon zrobił to później, gdy było już ich mało. Dlatego musiał skupywać małe pule tych adresów. Dlatego lista zakresów IP w pliku od Amejzona jest b. długa. Jej załadowanie do UFW trwa chyba ponad godzinę (piszę „chyba ponad godzinę" bo tylko raz spróbowałem odblokować w UFW Amejzona, to się udało ale trwało b. długo).

Nie jest to jedynie niezręczność, bo wiele innych s. WWW nie wiedzieć po co odwołuje się do dostawców chmurowych takich jak Amejzon.

W dodatku sklep Amejzon do prawidłowego działania powinien wymagać małej puli adresów IP.

11.1.7 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 Amejzon), 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 podali mi s. z tymi adresami: https://foundation.wikimedia.org/wiki/Archive:Wikipedia_Zero . Natomiast 2023-09-28, czw. zauważyłem, że wikipedia.org używa nie zadeklarowanego adresu IP 185.15.59.224. Gdy o to spytałem, odp. mi „The Wikpedia Zero project has been retired, we no longer maintain that list: https://foundation.wikimedia.org/wiki/Archive:Wikipedia_Zero".

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. i możliwe było by spr. jakie wymagania ma dana s. 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 wikpiedia.org) dokonuje ataków krakerskich.

Dlatego nigdy nie należy używać adresu wikipedia.pl do wchodzenia na pl.wikipedia.org .

11.2 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.

11.3 Przeglądarka Tor[59]

Przeglądarka Tor to zmodyfikowana przeglądarka Ognisty Lis. Usunięto z niej kod odpowiedzialny za śledzenie i dodano klienta sieci Tor.

Sieć Tor (z którego korzysta Przeglądarka Tor) 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 Przeglądarka Tor
- Przeglądarka Tor 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 samodzielne 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 Ogniste Więzienie.

Wielkie korpo szykanują użytkowników sieci Tor (po prostu odrzucając ruch ze wszystkich końcówek sieci Tor).

Ja osobiście nie korzystam już z sieci Tor z tego powodu, że nie ma możliwości określenia jednego p. wejścia do tej sieci (jego IP), a to powoduje brak kontroli nad ruchem wychodzącym (UFW), a to jest niedopuszczalne.

Z koli sens 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.

59 W j. ang.: Tor Browser

11.4 Przeglądarka Wodny Lis[60]

Wodny Lis to zmodyfikowana przeglądarka FireFox. Usunięto z niej kod odpowiedzialny za śledzenie. Dodatkowo ma ona wsparcie dla starszych wtyczek używanych dawniej w FireFox.

Paczka dla sys. Linuks ma postać zwykłego archiwum bzip2. Dlatego wystarczy ją pobrać, rozpakować i skopiować do katalogu $HOME.

Gdy używasz Wodny Lis na partycji z kat. $HOME nie może ona być montowana z flagą noexec (plik /etc/fstab).

Z przeglądarki Wodny Lis nie należy korzystać, bo nie działa ona w piaskownicy Ogniste Więzienie (czyli szpieguje użytkowników i kradnie ich dane).

Z przeglądarki Wodny Lis nie należy korzystać, bo brak możliwości wpłacania pieniędzy za jej użycie (czyli ma generować kwity bankowe jakich nie można w żaden normalny sposób spłacić).

11.5 Poprawa prywatności w Przeglądarce Tor, Wodny Lis i Ognisty Lis

Przeglądarka Tor i Wodny Lis to w pełni kompatybilne warianty Ognisty Lis.

Wszystkie rozszerzenia z Ognisty Lis działają w Przeglądarka Tor i Wodny Lis.

Rozszerzenia z Chrome nie działają w Ognisty Lis.

Często rozszerzenia mają odrębne wersje dla Chrome i dla Ognisty Lis.

11.5.1 Włącz kasowanie ciasteczek przy zamykaniu

11.5.2 Włącz kasowanie całej historii przy zamykaniu

11.5.3 Zainstaluj dodatek HTTPS Everywhere

Ten dodatek powoduje, że przeglądarka (gdy ma taką możliwość) to faworyzuje szyfrowane połączenia czyli HTTPS.

11.5.4 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 instalowaniu przeglądarki i jej dodatków należy starannie przejrzeć wszystkie ich opcje.

11.6 Przeglądarka Chromium

Chromium to Chrome bez śledzenia. Czyli Chromium dla Chrome jest tym co Wodny Lis dla Ognisty Lis.

Jest możliwość wejścia do sieci Tor przez Chromium i Chrome ale to wymaga kompilacji pakietu Tor ze źródeł i instalacji odpowiedniej wtyczki[61].

Aby zainstalować Chromium należy wydać polecenia:

- W Debianie:

```
sudo apt update
sudo apt install snapd
sudo snap refresh
sudo snap install chromium
```

- W Ubuntu

60 W j. ang.: Waterfox

61 Jest to opisane tu: https://www.techrepublic.com/article/how-to-install-tor-for-chrome-for-even-more-private-browsing .

```
sudo snap install chromium
```

Z przeglądarki Chromium nie należy korzystać, bo nie działa ona w piaskownicy Ogniste Więzienie (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).

11.7 Poprawa prywatności w Chromium i Chrome

Chromium to w pełni kompatybilny klon Chrome.

W Chromium działają wszystkie rozszerzenia Chrome.

Rozszerzenia z Ognisty Lis nie działają w Chrome.

Często rozszerzenia mają odrębne wersje dla Chrome i dla Ognisty Lis.

11.7.1 Włącz kasowanie ciasteczek przy zamykaniu

11.7.2 Włącz kasowanie całej historii przy zamykaniu

11.7.3 Zainstaluj dodatek HTTPS Everywhere

Ten dodatek powoduje, że przeglądarka (gdy ma taką możliwość) to faworyzuje szyfrowane połączenia czyli HTTPS.

11.7.4 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 instalowaniu przeglądarki i jej dodatków należy starannie przejrzeć wszystkie ich opcje.

11.7.5 Autouzupełniaj wyszukiwania i adresy URL

Wyłącz to na stronie:

```
chrome://settings/syncSetup
```

11.7.6 Ulepsz wyszukiwanie i przeglądanie

Wyłącz to na stronie:

```
chrome://settings/syncSetup
```

11.7.7 Wyczyść pliki cookie i dane witryn w momencie zamknięcia Chromium/Chrome

Włącz to na stronie:

```
chrome://settings/cookies
```

11.7.8 Wysyłaj żądanie „Bez śledzenia” podczas przeglądania

Włącz to na stronie:

```
chrome://settings/cookies
```

11.7.9 Kontynuuj działanie aplikacji w tle po zamknięciu Chromium

Wyłącz to na stronie:

```
chrome://settings/privacy
```

11.8 Wyłączenie obsługi JavaScript w przeglądarkach

Nie zalecam. Bo jak się wyłączy Java Script to ciągle trzeba go włączać by móc normalnie korzystać z funkcji stron WWW. Jak chcesz się przekonać, to:

11.8.1 Przeglądarka Tor, Wodny Lis, Ognisty Lis

W przypadku Przeglądarka Tor zalecam najpierw usunięcie dodatku NoScript.

Zainstaluj dodatek Disable JavaScript i ikoną obok paska adresu włączasz i wyłączasz JavaScript globalnie.

11.8.2 Chromium, Chrome

JavaScript wyłączasz w opcjach globalnie na s.:

```
chrome://settings/content/javascript
```

i włączasz go w razie potrzeby dla wybranej stronie ikonką na pasku adresu.

11.9 Inne przydatne dodatki

11.9.1 I don't care about cookies

11.9.1.1 Przeglądarka Tor, Wodny Lis i Ognisty Lis

https://addons.mozilla.org/en-US/firefox/addon/i-dont-care-about-cookies/ ;

11.9.1.2 Chromium i Chrome

https://chrome.google.com/webstore/detail/i-dont-care-about-cookies/fihnjjcciajhdojfnbdddfaoknhalnja .

11.9.2 Otwieranie linku i przejście do nowej karty jednym mlaskiem środkowego przycisku myszy

11.9.2.1 Przeglądarka Tor, Wodny Lis i Ognisty Lis

Otwierasz stronę konfiguracji:

```
about:config
```

I zmieniasz: browser.tabs.loadInBackground = true na: browser.tabs.loadInBackground = false

11.9.2.2 Chromium i Chrome

Zainstaluj dodatek:

```
https://chromewebstore.google.com/
detail/tab-activate/
jlmadbnpnnolpaljadgakjilggigioaj
```

11.10 Wyszukiwarki

11.10.1 Google.com

Tu mamy czasem lepsze wyniki wyszukiwania niż w DuckDuckGo.com .

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 z odpowiednią przeglądarką:

Chrome + Firejail + Google.com .

11.10.2 DuckDuckGo.com

Zaletą tej wyszukiwarki jest to, że nie śledzi oraz to, że nie szykanuje użytkowników sieci Tor. Do prostych zapytań jest wystarczająca (jednak nie do wszystkich).

Dla mnie sieć Tor dyskwalifikuje nie znane IP bramki tej sieci, co powoduje brak możliwości blokady ruchu wychodzącego w UFW.

Dlatego na co dzień używam:

Chrome + Firejail + DuckDuckGo.com .

12 Lektura uzupełniająca

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

13 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.
4. **Ograniczenia licencji nie dotyczą autora.**