Kurs administrowania systemem Linux 2022

Lista zadań na pracownię nr 6

Na zajęcia 11 i 13 kwietnia 2022

Przeczytaj uważnie wymienione w poniższych zadaniach strony podręcznika systemowego, a następnie wykonaj podane czynności administracyjne i przygotuj krótkie omówienie użytych poleceń (własnymi słowami — nie kopiuj podręcznika systemowego!) oraz tego, co udało się wykonać i z czym były problemy.

Zadanie 1 (1 pkt).

1. Załóż w swoim systemie nowego użytkownika: `Jan Testowy <jantest>`. Jeśli używasz Debiana, skorzystaj z wysokopoziomowych narzędzi, takich jak `adduser(8)`. W innych systemach wybierz narzędzie oferowane przez Twoją dystrybucję. W ostateczności użyj niskopoziomowych poleceń typu `useradd(8)`.
2. Zapisz go do odpowiednich grup tak, aby mógł korzystać z takich urządzeń, jak CD-ROM, akceleracja grafiki, dźwięk, interfejs bluetooth itp. Uwaga: nie wszystkie dystrybucje Linuksa wykorzystują mechanizm grup do nadawania użytkownikom uprawnień dostępu do urządzeń. Omów wówczas mechanizm użyty w Twojej dystrybucji.
3. Udostępnij mu za pomocą mechanizmu `sudo(8)` możliwość uruchamiania polecenia `ip(1)` jako użytkownik `root`.
4. Utwórz grupę `projekt` i zapisz do niej siebie oraz Jana. Utwórz plik `opis.txt` i nadaj mu grupę `projekt` oraz odpowiednie prawa dostępu tak, żebyście wspólnie z Janem mogli go edytować, ale żeby był całkowicie niedostępny dla innych użytkowników. Sprawdź, że faktycznie obaj macie do niego dostęp.
5. Sprawdź za pomocą polecenia `groups(1)` do jakich grup należysz, a do jakich grup należy Jan.
6. Daj Janowi możliwość uruchamiania polecenia `whoami(1)` jako Ty (nie jako `root`). Sprawdź, co zostanie wypisane, jeśli Jan uruchomi to polecenie za pomocą `sudo` żądając zmiany użytkownika na Twoje konto.
7. Skonfiguruj system tak, aby użytkownik `jantest` mógł samodzielnie zmienić swoje imię i nazwisko. Zaloguj się na konto `jantest`. Zmień informacje GECOS tego konta.

Zadanie 2 (1 pkt). Zapoznaj się z dokumentacją systemu kontroli wersji GNU RCS i przygotuj jego omówienie. Użyj tego systemu do kontroli wersji pliku `opis.txt` z punktu 4. poprzedniego zadania. Wykonaj ciąg zmian na przemian jako Ty i jako użytkownik `jantest`. Przetestuj wykluczanie dostępu do tego pliku po jego wypożyczeniu (ang. *checkin*) itp. Uwaga: w porównaniu do Git-a, RCS wydaje się bardzo siermiężny, ale jest często używany tam, gdzie potrzebne jest proste i lekkie rozwiązanie, np. do kontroli wersji plików w katalogu `/etc/`.

Zadanie 3 (2 pkt).

1. Sprawdź, czy na Twoim komputerze działa serwer `ssh` (i jeśli zachodzi taka potrzeba, uruchom go).
2. Wygeneruj za pomocą `ssh-keygen(1)` parę 4096-bitowych kluczy RSA[1] o nazwie `dojana`. Pamiętaj o ustawieniu dostatecznie trudnego hasła dostępu do klucza prywatnego!

[1] Klucze RSA są obecnie uważane za przestarzałe. W nowszych instalacjach domyślnie generowane są klucze bazujące na krzywych eliptycznych, takie jak ECDSA i EdDSA (Ed25519).

3. Za pomocą `ssh-copy-id(1)` skopiuj klucz publiczny `dojana.pub` na konto `jantest@localhost`. Sprawdź, że podając ten klucz w poleceniu `ssh(1)` możesz się zalogować na konto `jantest` bez potrzeby uwierzytelniania hasłem (podajesz tylko hasło do odblokowania klucza prywatnego).
4. Skonfiguruj parametry logowania na konto `jantestowy@localhost` w pliku `ssh_config(5)` tak, by móc wygodnie się logować bez potrzeby podawania wszystkich parametrów logowania.
5. Użyj polecenia `ssh-add(1)` w celu spamiętania na najbliższe 60 minut klucza prywatnego `dojana`. Zobacz, że w bieżącej sesji możesz łączyć się za pomocą `ssh` z kontem `dojana` bez potrzeby uwierzytelniania. Usuń następnie spamiętany klucz prywatny z pamięci `ssh-agenta`.
6. Zablokuj hasło użytkownika `jantest`. Sprawdź, że uwierzytelnianie za pomoca hasła nie działa, ale dalej możesz korzystać z uwierzytelnienia kluczem RSA.
7. Dodaj sobie możliwość wykonywania dowolnych poleceń jako `jantest` za pomocą `sudo`. Sprawdź, że `sudo` na konto `jantest` działa, mimo że jego hasło jest zablokowane.
8. Odblokuj hasło użytkownika `jantest`. Sprawdź, że uwierzytelnianie hasłem działa. Zablokuj konto `jantest`. Sprawdź, że żadna metoda uwierzytelniania (hasło, `sudo`, `ssh` z kluczem RSA) nie działają.
9. Odblokuj konto `jantest`. Zmień jego domyślną powłokę na `/bin/false`. Sprawdź, że polecenie `sudo` dla tego konta nadal działa, ale nie można zalogować się w konsoli (bezpośrednio lub poprzez `su`), ani poprzez `ssh`. Do czego służy polecenie `nologin(8)` i kiedy lepiej je używać zamiast `false(1)`?
10. Sprawdź, jak można zablokować logowanie się na konto `root` poprzez `ssh`, pozostawiając możliwość logowania się w konsoli.
11. Sprawdź, jak można zablokować uwierzytelnianie hasłem w `ssh`, pozostawiając tę możliwość podczas logowania w konsoli.

Zadanie 4 (1 pkt). Zapoznaj się z dokumentacją polecenia `newusers(8)` i przygotuj krótkie jego omówienie. Użyj go, by jednym poleceniem założyć następujących użytkowników (przyjmij, że niewymienione parametry powinny być domyślne):

- Anomalia Nowak, *username:* `anowak`, *password:* `polska123`;
- Katarzyna Kowalska, *username:* `kko`, hasło zablokowane;
- Jan Niezbędny, *username:* `jann`, *password:* `qwerty`, *shell:* `rbash`;
- Motion Daemon, username: `motiond`, hasło zablokowane, *shell:* `false`.

Dowiedz się, do czego służy powłoka `rbash`. Na koniec usuń założone konta. W Debianie użyj polecenia `deluser(1)`, w innych dystrybucjach — narzędzi, które one oferują.

Zadanie 5 (1 pkt). Dowiedz się, jak działają w Linuksie *terminale wirtualne* (VT) i jakie pliki reprezentują je w pseudosystemie `/dev`, co robi demon `getty(8)`, jakimi skrótami klawiszowymi można się przełączać pomiędzy terminalami wirtualnymi oraz jakie są linuksowe zwyczaje dotyczące ich tworzenia i użycia. Utwórz użytkowników `user13` i `user42`. Skonfiguruj system tak, aby podczas uruchamiania systemu `user13` był automatycznie zalogowany na terminalu `tty8`, zaś `user42` — na terminalu `tty9`.

Zadanie 6 (2 pkt). Zainstaluj w swoim systemie jakiegoś prostego zarządcę okien (dobrym wyborem jest np. Openbox). Skonfiguruj użytkownika `user13` z poprzedniego zadania tak, aby poleceniem `startx` wydanym w terminalu wirtualnym mógł uruchomić na nim zarządcę okien (niezależnie od systemów okienkowych działających na innych terminalach). Zauważ, że na terminalu `tty8` możesz teraz używać systemu okienkowego odizolowanego od Twojego normalnego systemu. Uruchamianie niezaufanych aplikacji okienkowych jest w takim systemie znacznie bezpieczniejsze (szczególnie, jeśli używasz Xorg — Wayland zapewnia nieco lepszą ochronę). Dodaj następnie do `.profile` polecenie, aby po automatycznym zalogowaniu użytkownika `user13` w terminalu `tty8` automatycznie uruchamiał się zarządca okien (ale tylko wówczas, więc polecenie `startx` wywołuj warunkowo). Zauważ, że możesz dzięki temu automatycznie logować i uruchamiać zarządcę okien bez potrzeby używania graficznego zarządcy logowania (takiego, jak xdm).

Zadanie 7 (1 pkt). Zapoznaj się z podstawowymi opcjami poleceń `ip link(1)` i `ip addr(1)`, w szczególności

```
ip link set device [up | down]
ip addr [add | del] address/mask dev device
ip addr flush dev device
ip addr show dev device
```

Połącz gniazda ethernetowe dwóch komputerów kablem. Zadanie możesz wykonać wraz z kolegą. Uruchom(cie) i skonfiguruj(cie) interfejsy sieciowe obu komputerów tak, by możliwa była ich komunikacja. Zadanie możesz również wykonać w maszynach wirtualnych.

Zadanie 8 (1 pkt). Przygotuj odpowiednią konfigurację połączenia z poprzedniego zadania w pliku `interfaces(5)`. Zobacz, jak wygodnie możesz konfigurować i dekonfigurować interfejs za pomocą poleceń `ifup(8)` i `ifdown(8)`.

Zadanie 9 (1 pkt). Połącz się z drugim komputerem za pomocą interfejsów WiFi. Skonfiguruj je w trybie *ad hoc*. Użyj polecenia `iw(8)` oraz `iwconfig(8)`.

Zadanie 10 (1 pkt). Zapoznaj się z demonem `wpa_supplicant(8)` i poleceniem `wpa_cli(8)`. Skonfiguruj połączenie z punktem dostępowym zabezpieczonym protokołem WPA 2 Personal, w szczególności przygotuj odpowiedni plik konfiguracyjny dla WPA Supplicanta. Dodaj odpowiednie wpisy do pliku `/etc/network/interfaces/` tak, żeby można było włączać i wyłączać interfejs WiFi za pomocą poleceń `ifup` i `ifdown`.