Kurs administrowania systemem Linux 2019

Lista zadań na pracownię nr 7

Na zajęcia 8 kwietnia 2019

Przeczytaj uważnie wymienione w poniższych zadaniach strony podręcznika systemowego, a następnie wykonaj podane czynności administracyjne i przygotuj się do zaprezentowania ich podczas zajęć.

Zadanie 1 (1 pkt).

- Załóż w swoim systemie nowego użytkownika: `Jan Testowy <jantest>`.
- Zapisz go do odpowiednich grup tak, aby mógł korzystać z takich urządzeń, jak CD-ROM, kamera internetowa, interfejs bluetooth itp.
- Udostępnij mu za pomocą mechanizmu `sudo(8)` możliwość uruchamiania polecenia `ip(1)` jako użytkownik `root`.
- 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.
- Sprawdź za pomocą polecenia `groups(1)` do jakich grup należysz, a do jakich grup należy Jan.
- 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.
- 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 (2 pkt).

- Sprawdź, czy na Twoim komputerze działa serwer `ssh` (i jeśli zachodzi taka potrzeba, uruchom go).
- Wygeneruj za pomocą `ssh-keygen(1)` parę 4096-bitowych kluczy RSA o nazwie `dojana`. Pamiętaj o ustawieniu dostatecznie trudnego hasła dostępu do klucza prywatnego!
- 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).
- Skonfiguruj parametry logowania na konto `jantestowy@localhost` w pliku `ssh_config(5)` tak, by móc wygodnie się logować bez potrzeby podawania wszystkich parametrów logowania.
- 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`.
- Zablokuj hasło użytkownika `jantest`. Sprawdź, że uwierzytelnianie za pomoca hasła nie działa, ale dalej możesz korzystać z uwierzytelnienia kluczem RSA.
- Dodaj sobie możliwość wykonywania dowolnych poleceń jako `jantest` za pomocą `sudo`. Sprawdź, że `sudo` na konto `jantest` działa, mimo że jego hasło jest zablokowane.

- 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.
- Odblokuj konto `jantest`. Zmień jego domyślną powłokę na `/bin/false`. Sprawdź, że polecenia `su` i `sudo` dla tego konta nadal działają, ale nie można zalogować się na konsoli, ani poprzez `ssh`. Do czego służy polecenie `nologin(8)` i kiedy lepiej je używać zamiast `false(1)`?
- Sprawdź, jak można zablokować logowanie się na konto `root` poprzez `ssh`, pozostawiając możliwość logowania się na konsoli.

Zadanie 3 (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. W razie braku kabel sieciowy możesz pożyczyć od prowadzącego. Uruchom(cie) i skonfiguruj(cie) interfejsy sieciowe obu komputerów tak, by możliwa była ich komunikacja. Zadanie możesz również wykonać w maszynach wirtualnych.

Zadanie 4 (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 5 (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 6 (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. W takcie zajęć będzie dostępny w pracowni mały domowy punkt dostępowy.