Politechnika Śląska

Sprawozdanie z modułu nr 2

BSKiST 2022/2023

Bezpieczeństwo sieci komputerowych i systemów teleinformatycznych

Kierunek: Informatyka

Członkowie zespołu:
Grzegorz Koperwas

Gliwice, 2022/2023

Spis treści

1 Wprowadzenie

1.1 Zespół projektowy

Grzegorz Koperwas :: Wszystko

1.2 Wprowadzenie

Omawianym w tej pracy rozwiązaniem dostarczającym usługi kryptograficzne będzie program `GnuPG`. Dodatkowo zostanie omówiony mechanizm uwierzytelniania użytkowników `PAM` w kernelu Linux'a.

Oprócz tego zostanie omówione wdrażanie wirtualnej sieci prywatnej w oparciu o program `OpenVPN` na systemie `GNU/Linux`.

2 Rozwinięcie

2.1 GnuPG

Program `GnuPG` jest dostępny w praktycznie każdej dystrybucji systemu `Gnu/Linux`, na przykład w dystrybucji `Arch` możemy zainstalować go za pomocy komendy `pacman -S gpg`.

W celu korzystania z programu należy wygenerować lub dodać istniejący klucz prywatny. By wygenerować klucz należy użyć opcji `--full-generate-key`. Następnie należy wybrać algorytm do którego będzie służył klucz, jego wielkość oraz jak długo powinien obowiązywać.

`GnuPG` pozwala nam dokonywać wszystkich powszechnych operacji kryptograficznych, takich jak:

- Symetryczne szyfrowanie plików za pomocą hasła.
- Szyfrowanie oraz podpisywanie asymetryczne, gdzie znając klucz publiczny odbiorcy możemy wysłać mu wiadomość którą tylko on może otworzyć.
- Zarządzanie prywatnymi oraz publicznymi kluczami - Możemy zarządzać oraz używać kluczy prywatnych zapisanych na kartach inteligentnych `OpenPGP` oraz zarządzać poziomem zaufania do zapisanych kluczy publicznych innych użytkowników.

  `GnuPG` również implementuje rozwiązanie *Web-of-trust*, które jest realizowane poprzez gromadzenie podpisów kluczy publicznych danej osoby przez innych użytkowników. Na przykład jeżeli ufamy osobie A, a osoba A ufa osobie B, to nasz system automatycznie ufa osobie B.

2.2 PAM

Kernel Linux'a zawiera wbudowany system zarządzania procesem autoryzacji użytkowników. `Linux Pluggable Authentication Modules` pozwala na zarządzanie jakie metody uwierzytelniania są wystarczające dla danych akcji.

`PAM` jest częścią kernela, więc instalacja nie jest konieczna.

Konfigurowanie `PAM` jest realizowane poprzez pliki umieszczone w katalogu `/etc/pam.d/`. Dla każdego programu, który wymaga autoryzacji użytkowników (np. Blokada ekranu `swaylock` czy polecenie `sudo`) jest dostępny plik, który pozwala na konfigurację metod uwierzytelniania dla danego programu.

Przykładowo dla programu `swaylock` możemy wymagać autoryzacji poprzez czytnik linii papilarnych, a dla deamona `sshd`, z powodu trudności z obsługą biometrii zdalnie, możemy wymagać hasła oraz kodu z aplikacji *google authenticator*.

2.3 OpenVPN

OpenVPN jest oprogramowaniem VPN, które pozwala na bezpieczne połączenie z siecią prywatną poprzez publiczne połączenie internetowe. Można go skonfigurować w celu uzyskania dostępu do zasobów sieciowych i aplikacji, które normalnie są niedostępne poza siecią. OpenVPN jest elastyczny i można go skonfigurować do pracy z różnymi protokołami, takimi jak TCP i UDP, i jest w stanie pracować z różnymi systemami operacyjnymi, w tym Windows, macOS, iOS i Android.

Możemy zainstalować zarówno serwer jak i klient OpenVPN komendą `pacman -S openvpn`. Konfigurację serwera openvpn najlepiej jest utworzyć na podstawie domyślnego, okomentowanego configu oraz umieścić ją w folderze `/etc/openvpn/server`.

Odpowiednio skonfigurowany serwer uruchamiamy jako deamon za pomocą `systemd enable --now openvpn-server@<config>`.