

Zadanie to dotyczy instalacji, konfiguracji i uruchamiania firewalla (iptables) w systemie operacyjnym Linux, zwłaszcza na platformie Ubuntu. Poniżej znajdziesz wnioski, które uczniowie powinni wyciągnąć z poszczególnych części zadania:

Wnioski z każdej części zadania:

A. Zapoznanie z iptables

1. Funkcje iptables:

- **INPUT:** Pakiety przychodzące do komputera.
- **OUTPUT:** Pakiety generowane przez komputer.
- **FORWARD:** Pakiety przekazywane przez komputer.
- **ACCEPT:** Akceptuje pakiet.
- **DROP:** Odrzuca pakiet.
- **REJECT:** Odrzuca pakiet i odsyła z powrotem do nadawcy.

2. System V vs. SystemD:

- System V (Sysvinit) to starszy system inicjalizacji.
- SystemD jest nowszym systemem, zastępującym System V.
- Sprawdzenie używanego systemu: **systemd --version** lub **dpkg -S /sbin/init**.

B. Tworzenie skryptu firewalla dla System V

1. Tworzenie skryptu:

- Skrypt firewalla jest uruchamiany podczas startu systemu.
- Plik `init.d/firewall` zawiera konfigurację iptables.
- Przykład reguł blokujących pewne połączenia.

2. Zarządzanie skryptem:

- **chmod +x /etc/init.d/firewall:** Nadanie praw do uruchamiania.
- **update-rc.d firewall defaults 90:** Ustawienia automatycznego uruchamiania.

3. Błędy skryptu:

- Komunikat **systemd-sysv-generator:** Ignorowanie aliasu `firewall.service`. Skrypt działa, ale nie jest dostosowany do systemd.

C. Usuwanie skryptu i skrypt zaawansowany

1. Usuwanie skryptu:

- **rm /etc/init.d/firewall:** Usunięcie skryptu.
- **update-rc.d firewall remove:** Usunięcie dowiązania.

2. Skrypt zaawansowany:

- Zaawansowane reguły blokujące skanowania i ataki DDoS.
- Logowanie odrzuconych pakietów.

D. Tworzenie skryptu firewala dla Systemd

1. Tworzenie skryptu:

- Skrypt uruchamiany przez systemd.
- Plik `/etc/systemd/system/firewall.service` definiuje usługę.

2. Uruchamianie usługi:

- **systemctl enable firewall.service:** Ustawienie autostartu.
- **systemctl start firewall.service:** Uruchomienie usługi.
- Sprawdzenie statusu: **systemctl status firewall.service.**

E. Ufw - frontend dla iptables

1. Ufw (Uncomplicated Firewall):

- Użyteczne narzędzie frontendowe dla iptables.
- Prosta konfiguracja i obsługa.

2. Instalacja i konfiguracja:

- **apt-get install ufw:** Instalacja ufw.
- Konfiguracja w `/etc/ufw/ufw.conf`.
- Możliwość obsługi protokołu IPv6.

Ogólne Wnioski:

- Iptables to potężne narzędzie do konfiguracji firewala w systemach Linux.
- System V i SystemD to różne systemy inicjalizacji, a wybór zależy od dystrybucji.
- Tworzenie skryptów startowych dla iptables może być zarówno dla System V, jak i SystemD.
- Ufw jest prostym frontendem ułatwiającym konfigurację iptables.

Zadanie to obejmuje cały proces instalacji, konfiguracji i uruchamiania iptables, a także przedstawia alternatywny sposób w postaci Ufw. Uczniowie powinni zrozumieć każdy krok tego procesu oraz zastosowanie iptables do zarządzania ruchem sieciowym i zabezpieczania systemu.