Firewall

written by archi | 21 marca 2021

Proszę wykonać całkowitą kontrolę wejścia TCP i UDP (odpowiednio) do serwera wirtualnego:

Porty otwarte dla komunikacji to: **22, 80 135, 137, 138, 139, 405, 443, 445, 10000**

wszystkie pozostałe próby komunikacji powinny zostać zablokowane wykorzystując akcję DROP.

W celu wykonania tego laboratorium uruchom w swoim systemie pakiet programowy WEBMIN lub wykonaj to wykorzystując komendy IPTABLES.

Przygotowanie pakietu webmin:

Podłącz się do swojego systemu wirtualnego z wykorzystaniem podłączenia szyfrowanego do terminala (`putty.exe`). Zaktualizuj bazę informacji o pakietach systemu oraz wykonaj upgrade systemu.

1. Otwórz stronę `http://www.webmin.com/download.html` i pobierz właściwy pakiet WEBMIN dla danego systemu operacyjnego (UBUNTU – DEBIAN) poprzez wybranie prawym przyciskiem myszy opcji „Kopiuj adres odnośnika” na linku. Następnie przy pomocy polecenia `wget` i wklejeniu skopiowanego linku (przy pomocy *SHIFT+prawy klawisz myszy*) pobierz oprogramowanie.

2. Używając polecenia dpkg zainstaluj pakiet webmin:

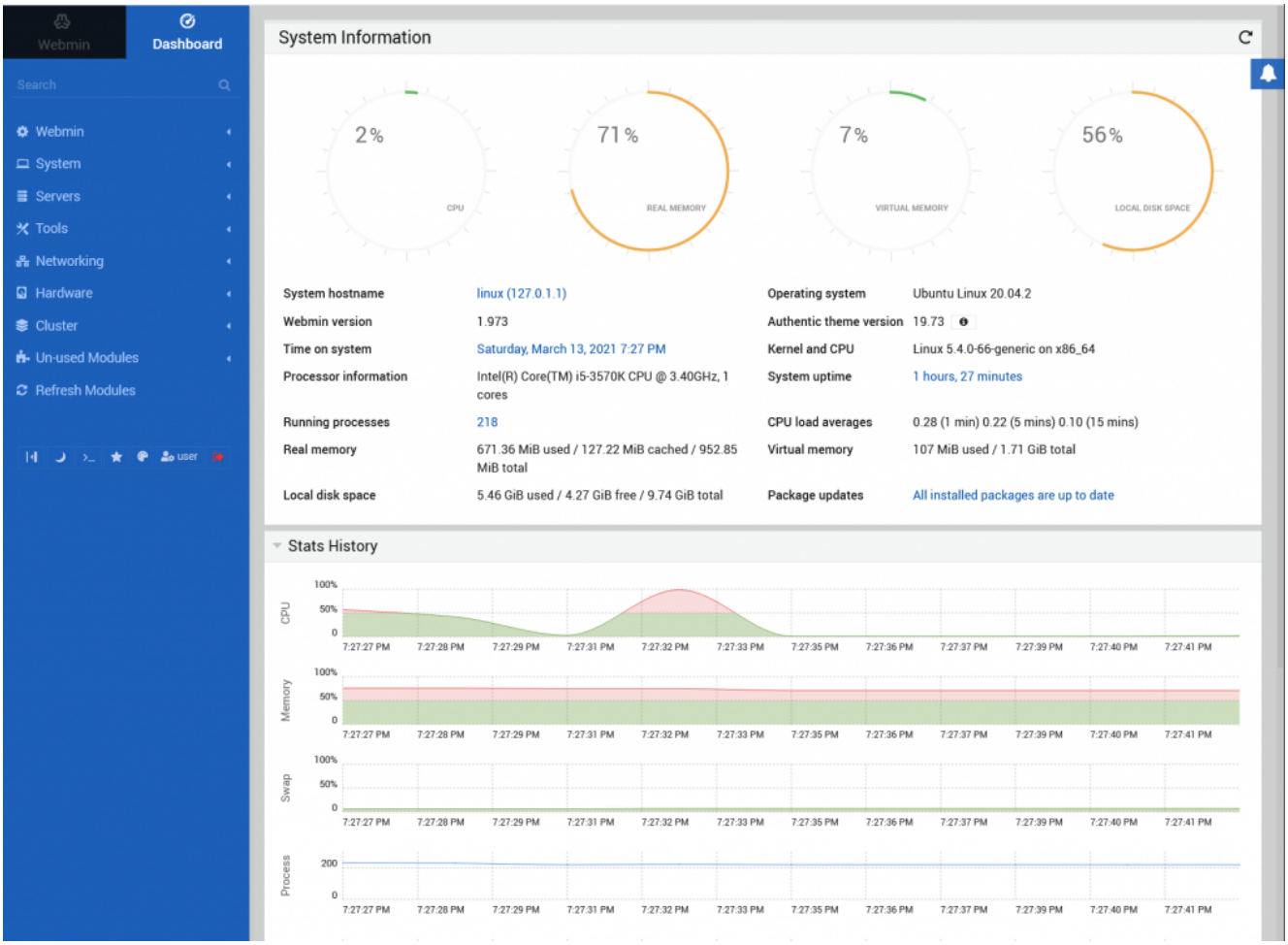
```
dpkg -i webmin_1.xxx_all.deb
```

3. Po instalacji mogą wystąpić problemy zależności miedzy pakietami. W celu ich rozwiązania należy wykonać polecenie:

```
apt install -f
```

4. Po instalacji zobaczysz na ekranie konsoli w jaki sposób podłączyć się do pakietu Webmin *(połącz się po https:// i port 10000 na swój ades IP)*.

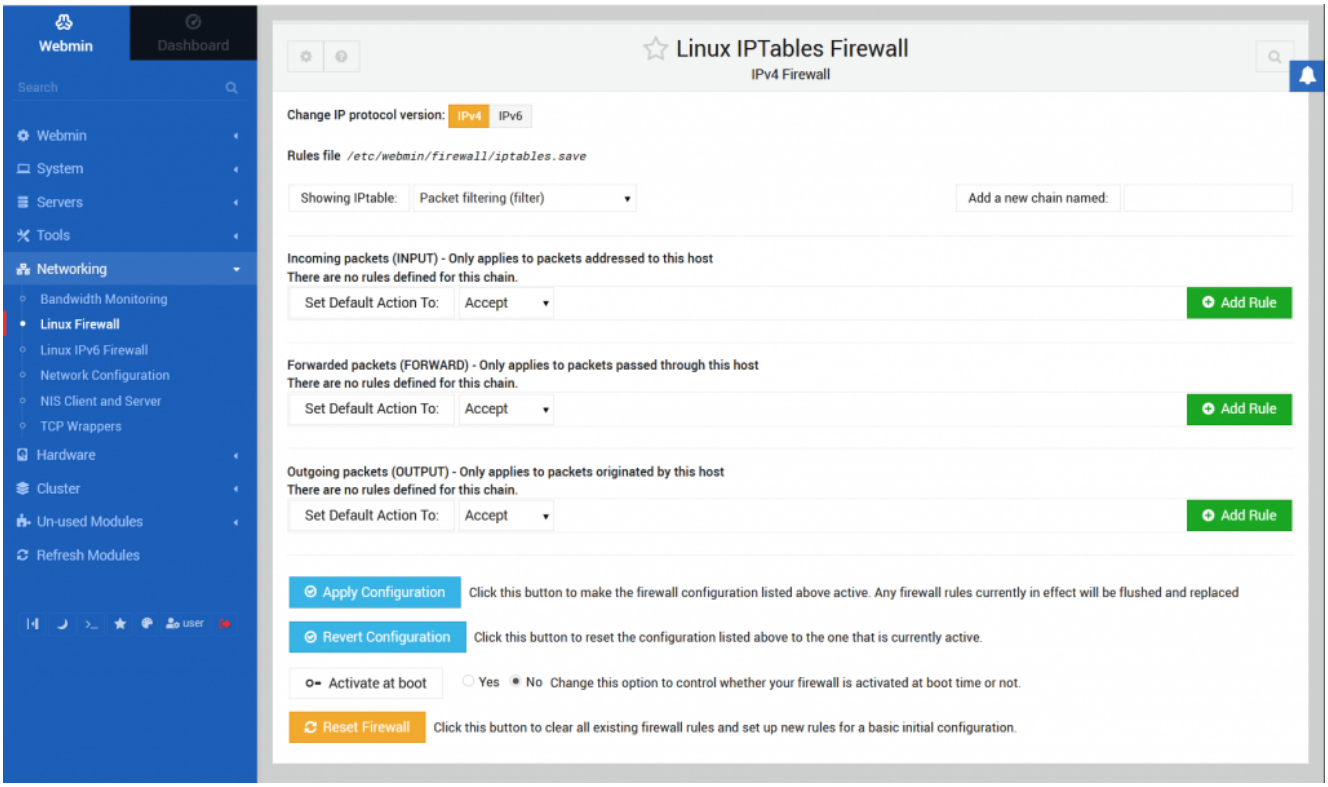
5. Po zalogowaniu się na użytkownika root (lub user) zobaczysz okno informacji o Twoim systemie. Informacja zawiera dane o kernelu, procesorze, pamięci, dysku oraz aktualizacji dla systemu. Z lewej strony znajduje się menu systemowe.



6. Otwórz w menu pozycje: Servers, Others, Networking.

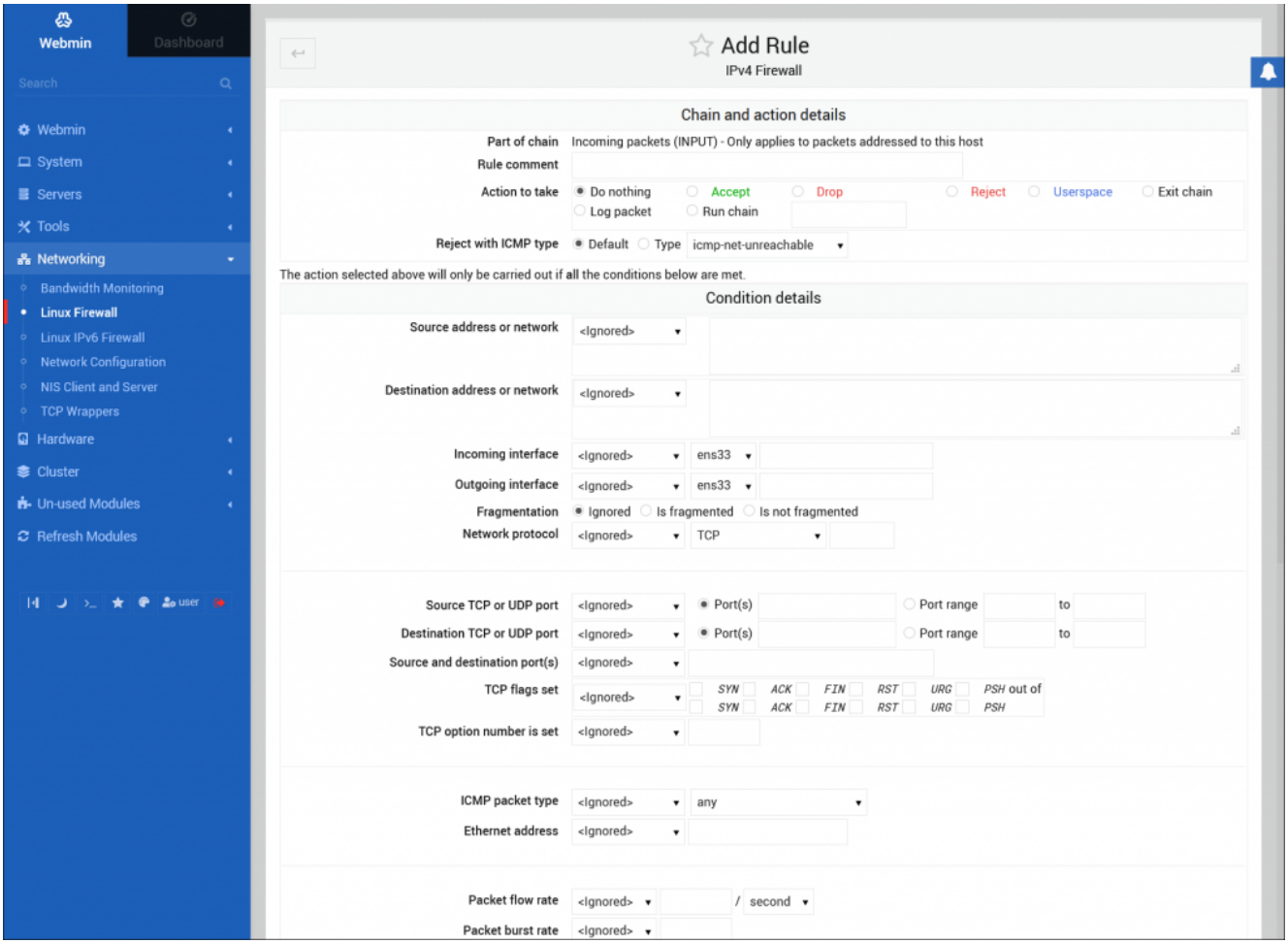
7. Zakładka Servers zawiera dostępne zainstalowane na serwerze usługi

pozwalając na ich konfigurację. Zakładka „Others” pozwala na zarządzanie dodatkami do systemu łącznie z uruchomieniem powłoki systemowej „shell”, zarządzaniem plikami „File Manager” oraz innymi ustawieniami. Zakładka Networking pozwala konfigurować ustawienia sieciowe, w tym zaporę systemową „Linux Firewall” – wybierz ją teraz właśnie.



8. Ustaw opcję „Activate at boot” na wartość **Yes**

9. Zapora nie posiada w chwili obecnej żadnych ustawień. Dozwolone są wszystkie połączenia. Zgodnie z założeniami laboratorium skonfiguruj dozwolone połączenia oraz blokady połączeń dokładnie w takiej kolejności. W tym celu w polu „Showing IPtable:” wybieramy „Packet filtering (filter)”. Następnie w sekcji „Incoming packets (INPUT)” dodajemy nową regułę naciskając przycisk „Add rule” zaraz poniżej po prawej stronie. Otworzy nam się okno konfiguracji reguły.



10. Kolejno wypełniamy tabele informacjami i zatwierdzamy przyciskiem na dole „Create”

11. Reguła pojawi się jako jedyna obecnie w opisie konfiguracji.

12. Powtarzaj kolejne dodawania od pkt. 9

13. Zapisanie i uaktywnienie stworzonych lub zmienianych reguł dokonuje się w ekranie głównym Firewall poprzez wybranie przycisku „Apply Configuration”.

15. Sprawdź ustawione reguły z wykorzystaniem polecenia w systemie `iptables -L`

Puste wpisy iptables

```
root@linux:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@linux:~# _
```

Wypełniona część reguł...

```
root@linux:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:webmin

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@linux:~# _
```