## **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.

O           Webmin         Dashboard           Search         Q	Linux IPTables Firewall				
Webmin     System     System     Servers     Tools     Metworking     Bandwidth Monitoring     Linux Firewall	Change IP protocol version: IPvi IPv6 Rules file /etc/webmin/Firewall/iptables.save Showing IPtable: Packet filtering (filter) Incoming packets (INPUT) - Only applies to packets addressed to this host There are no rules defined for this chain. Set Default Action To: Accept	d Rule			
Linux IPv6 Firewall  Network Configuration NIS Client and Server TCP Wrappers Hardware  Clienter	Forwarded packets (FORWARD) - Only applies to packets passed through this host There are no rules defined for this chain. Set Default Action To: Accept Outgoing packets (OUTPUT) - Only applies to packets originated by this host There are no rules defined for this chain.	d Rule			
<ul> <li>Crustel</li> <li>Modules</li> <li>G Refresh Modules</li> </ul>	Set Default Action To: Accept     Accept     Accept     Click this button to make the firewall configuration listed above active. Any firewall rules currently in effect will be flushed and replaced	i Rule			
-  J >_ ★ @ ≜suser 🗭	<ul> <li>Revert Configuration</li> <li>Click this button to reset the configuration listed above to the one that is currently active.</li> <li>Activate at boot</li> <li>Yes No Change this option to control whether your firewall is activated at boot time or not.</li> <li>Reset Firewall</li> <li>Click this button to clear all existing firewall rules and set up new rules for a basic initial configuration.</li> </ul>				

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.

A 0				
Webmin Dashboard	😭 Add Rule			
Search Q	IPv4 Firewall			
	Chain and action details			
≱ Webmin	in Incoming packets (INPIII) - Only applies to packets addressed to this bost			
⊐ System	nt			
Servers Action to take	e Do nothing Accept Drop Reject Userspace Exit chai			
Toole	O Log packet O Run chain			
Reject with ICMP type	Oefault O Type icmp-net-unreachable			
The action selected above will only be carried out	t if all the conditions below are met.			
Bandwidth Monitoring	Condition details			
Linux Pirewall Source address or network	rk <lgnored> •</lgnored>			
Network Configuration				
NIS Client and Server Destination address or network	rk <lanored></lanored>			
TCP Wrappers	Nginieux ·			
Hardware 🔹				
E Cluster	e <lgnored> • ens33 •</lgnored>			
Outgoing interfact	ce <lgnored> ▼ ens33 ▼</lgnored>			
Fragmentation	Ignored Is fragmented Is not fragmented			
Refresh Modules     Network protoco	ol <ignored> V ICP V</ignored>			
d J J S de Builder Inc.	the demonstration of Part (a)			
Source ICP or UDP por	tt kingnored> V Port(s) Port range to			
Destination TCP or ODP por	vitration of the second s			
Source and destination port(s				
TCP trags se	<pre>et <lgnored></lgnored></pre>			
TCP option number is se	et <lgnored> •</lgnored>			
ICMP packet type	<pre>elgnored&gt; v any v</pre>			
Ethernet address	ss <lgnored> •</lgnored>			
Packet flow rate	te <lgnored> • / second •</lgnored>			
Packet burst rate	te <lanored> •</lanored>			

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 root@linux:~# _	destination

Wypełniona część reguł...

root@linux:~# iptables –L						
Chain INPUT (pol	icy ACCEPT)					
target prot	opt source	destination				
ACCEPT tcp	anywhere	anywhere	tcp dpt:ssh			
ACCEPT top	anywhere	anywhere	tcp dpt:http			
ACCEPT top	–– anywhere	anywhere	tcp dpt:https			
ACCEPT top	-− anywhere	anywhere	tcp dpt:webmin			
Chain EORWARD (nolicy ACCEPT)						
target prot	opt source	destination				
Choin OUTPUT (policy ACCEPT)						
target prot opt source root@linux:~# _		destination				