

Jakub Jędrzejczak

PFsense:

```
The IPv4 LAN address has been set to 172.16.77.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
        https://172.16.77.1/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 7afe00985885b2615c61

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.5/24
LAN (lan)      -> em1      -> v4: 172.16.77.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM

Enter an option: █
```

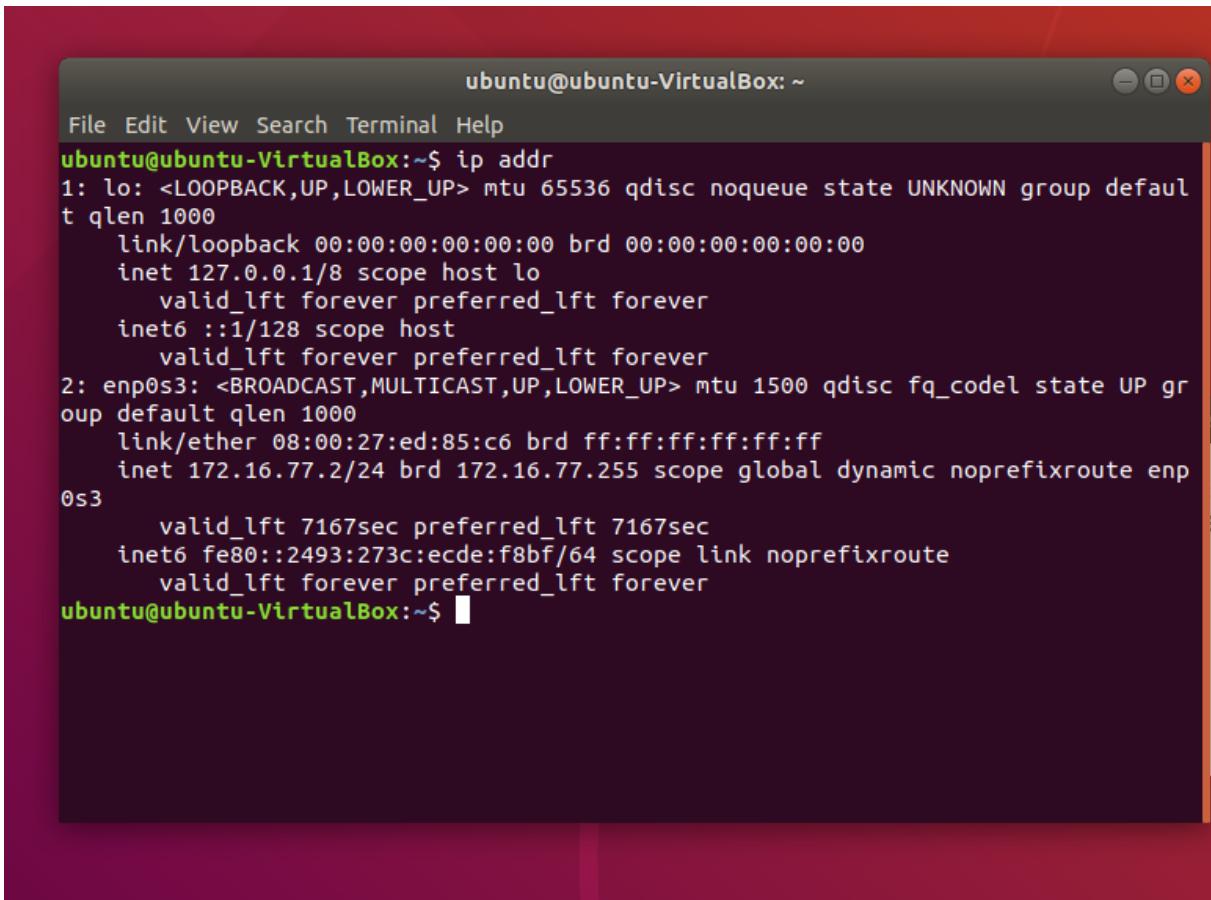
Kali:

```
root@kali:~#
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.1.6 netmask 255.255.255.0 broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fe50:4504 prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:50:45:04 txqueuelen 1000 (Ethernet)
            RX packets 312 bytes 63324 (61.8 KiB)
            RX errors 0 dropped 48 overruns 0 frame 0
            TX packets 74 bytes 6550 (6.3 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
            RX packets 20 bytes 1116 (1.0 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 20 bytes 1116 (1.0 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# █
```

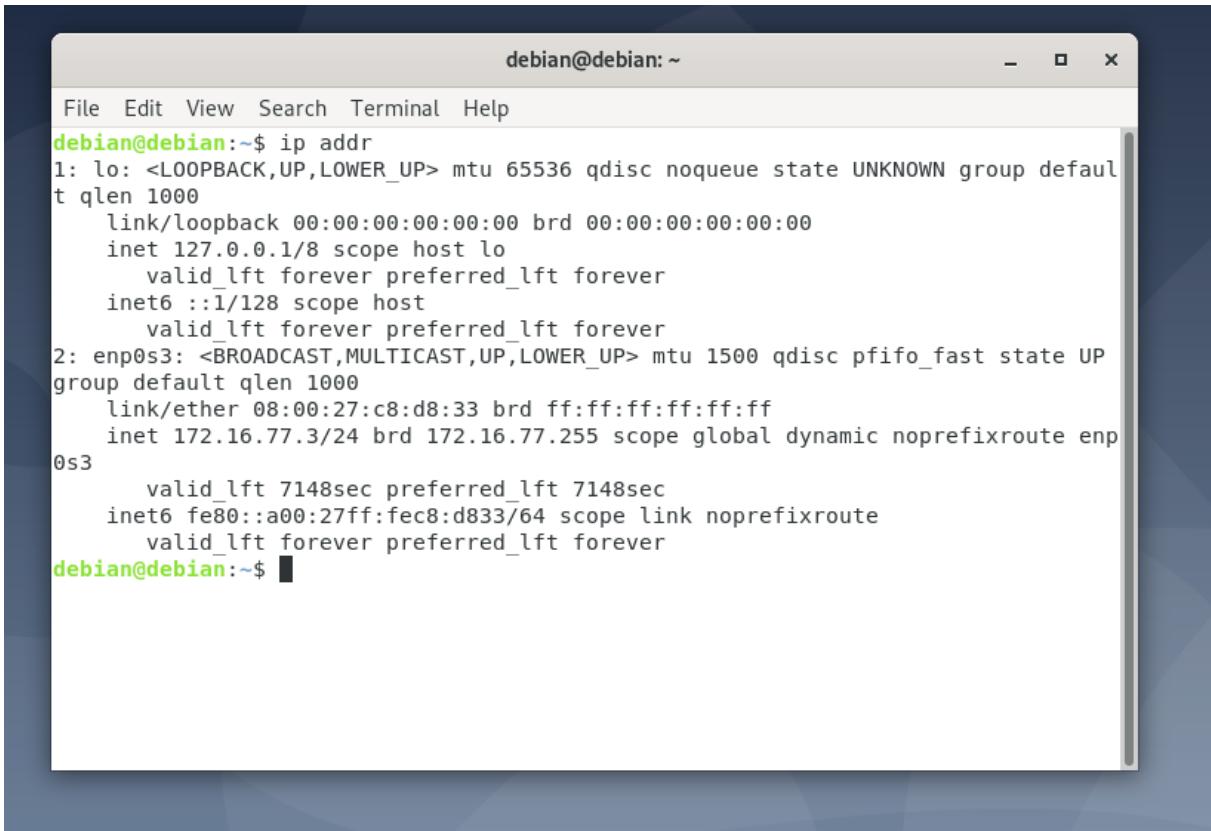
Ubuntu:



A screenshot of a terminal window titled "ubuntu@ubuntu-VirtualBox: ~". The window has a dark theme with white text. The terminal shows the output of the "ip addr" command. It lists two interfaces: "lo" (loopback) and "enp0s3" (ethernet). The "lo" interface has an IPv4 address of 127.0.0.1/8 and an IPv6 address of ::1/128. The "enp0s3" interface has an IPv4 address of 172.16.77.2/24 and an IPv6 address of fe80::2493:273c:ecde:f8bf/64. Both interfaces have a MTU of 1500 or 65536, a queueing discipline (qdisc) of fq_codel, and a state of UP. The "valid_lft" and "preferred_lft" values are set to forever for all interfaces.

```
ubuntu@ubuntu-VirtualBox:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ed:85:c6 brd ff:ff:ff:ff:ff:ff
    inet 172.16.77.2/24 brd 172.16.77.255 scope global dynamic noprefixroute enp0s3
        valid_lft 7167sec preferred_lft 7167sec
    inet6 fe80::2493:273c:ecde:f8bf/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
ubuntu@ubuntu-VirtualBox:~$
```

Debian:



The screenshot shows a terminal window titled "debian@debian: ~". The window contains the output of the command "ip addr". The output details two network interfaces: "lo" (loopback) and "enp0s3". The "lo" interface has an IPv4 address of 127.0.0.1/8. The "enp0s3" interface has an IPv4 address of 172.16.77.3/24 and an IPv6 address of fe80::a00:27ff:fe8:d833/64.

```
File Edit View Search Terminal Help
debian@debian:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:c8:d8:33 brd ff:ff:ff:ff:ff:ff
    inet 172.16.77.3/24 brd 172.16.77.255 scope global dynamic noprefixroute enp0s3
        valid_lft 7148sec preferred_lft 7148sec
    inet6 fe80::a00:27ff:fec8:d833/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
debian@debian:~$
```

Scenario Validation

1.

PFSense: 172.16.77.1/24

Kali: 192.168.1.6/24

Ubuntu: 172.16.77.2/24

Debian: 172.16.77.3/24

Windows: 192.168.1.3

2.

Version	2.6.0-RELEASE (amd64)
	built on Mon Jan 31 19:57:53 UTC 2022
	FreeBSD 12.3-STABLE

3.

```
Enter an option: 7
```

```
Enter a host name or IP address: 172.16.77.2
```

```
PING 172.16.77.2 (172.16.77.2): 56 data bytes  
64 bytes from 172.16.77.2: icmp_seq=0 ttl=64 time=0.187 ms  
64 bytes from 172.16.77.2: icmp_seq=1 ttl=64 time=0.203 ms  
64 bytes from 172.16.77.2: icmp_seq=2 ttl=64 time=0.170 ms
```

```
--- 172.16.77.2 ping statistics ---
```

```
3 packets transmitted, 3 packets received, 0.0% packet loss  
round-trip min/avg/max/stddev = 0.170/0.187/0.203/0.013 ms
```

```
Press ENTER to continue.
```

```
Enter an option: 7
```

```
Enter a host name or IP address: 172.16.77.3
```

```
PING 172.16.77.3 (172.16.77.3): 56 data bytes  
64 bytes from 172.16.77.3: icmp_seq=0 ttl=64 time=0.316 ms  
64 bytes from 172.16.77.3: icmp_seq=1 ttl=64 time=0.174 ms  
64 bytes from 172.16.77.3: icmp_seq=2 ttl=64 time=0.174 ms
```

```
--- 172.16.77.3 ping statistics ---
```

```
3 packets transmitted, 3 packets received, 0.0% packet loss  
round-trip min/avg/max/stddev = 0.174/0.221/0.316/0.067 ms
```

```
Press ENTER to continue.
```

4.

```
0> SMC#1
```

```
Enter an option: 7
```

```
Enter a host name or IP address: 192.168.1.3
```

```
Press ENTER to continue.

VirtualBox Virtual Machine - Netgate Device ID: 7afe00985885b2615c61

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.5/24
LAN (lan)      -> em1      -> v4: 172.16.77.1/24

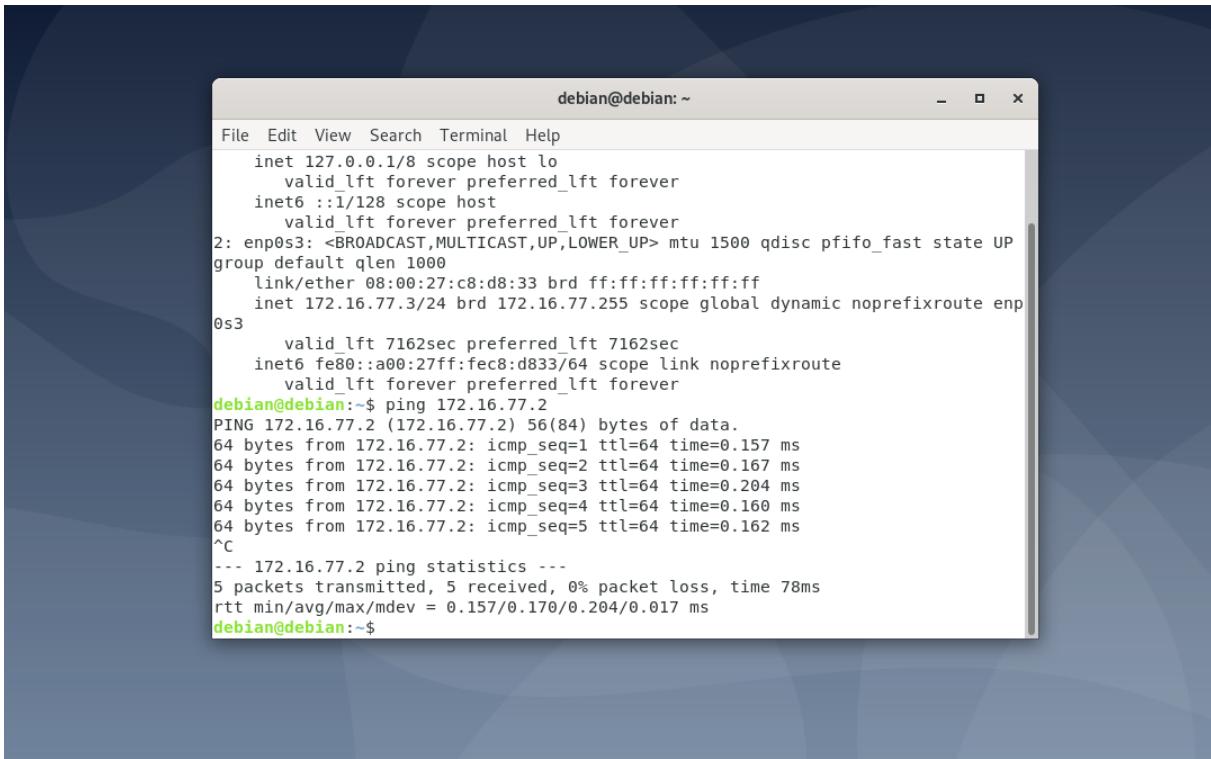
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 7

Enter a host name or IP address: 192.168.1.6
```

5.

```
File Edit View Search Terminal Help
ubuntu@ubuntu-VirtualBox:~$ ping 172.16.77.3
PING 172.16.77.3 (172.16.77.3) 56(84) bytes of data.
64 bytes from 172.16.77.3: icmp_seq=1 ttl=64 time=0.243 ms
64 bytes from 172.16.77.3: icmp_seq=2 ttl=64 time=0.259 ms
64 bytes from 172.16.77.3: icmp_seq=3 ttl=64 time=0.166 ms
64 bytes from 172.16.77.3: icmp_seq=4 ttl=64 time=0.173 ms
64 bytes from 172.16.77.3: icmp_seq=5 ttl=64 time=0.156 ms
64 bytes from 172.16.77.3: icmp_seq=6 ttl=64 time=0.162 ms
64 bytes from 172.16.77.3: icmp_seq=7 ttl=64 time=0.162 ms
^C
--- 172.16.77.3 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6149ms
rtt min/avg/max/mdev = 0.156/0.188/0.259/0.043 ms
ubuntu@ubuntu-VirtualBox:~$
```



The screenshot shows a terminal window titled "debian@debian: ~" running on a Linux system. The window displays the following output:

```
File Edit View Search Terminal Help
inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:c8:d8:33 brd ff:ff:ff:ff:ff:ff
    inet 172.16.77.3/24 brd 172.16.77.255 scope global dynamic noprefixroute enp0s3
        valid_lft 7162sec preferred_lft 7162sec
    inet6 fe80::a00:27ff:fec8:d833/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
debian@debian:~$ ping 172.16.77.2
PING 172.16.77.2 (172.16.77.2) 56(84) bytes of data.
64 bytes from 172.16.77.2: icmp_seq=1 ttl=64 time=0.157 ms
64 bytes from 172.16.77.2: icmp_seq=2 ttl=64 time=0.167 ms
64 bytes from 172.16.77.2: icmp_seq=3 ttl=64 time=0.204 ms
64 bytes from 172.16.77.2: icmp_seq=4 ttl=64 time=0.160 ms
64 bytes from 172.16.77.2: icmp_seq=5 ttl=64 time=0.162 ms
^C
--- 172.16.77.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 78ms
rtt min/avg/max/mdev = 0.157/0.170/0.204/0.017 ms
debian@debian:~$
```

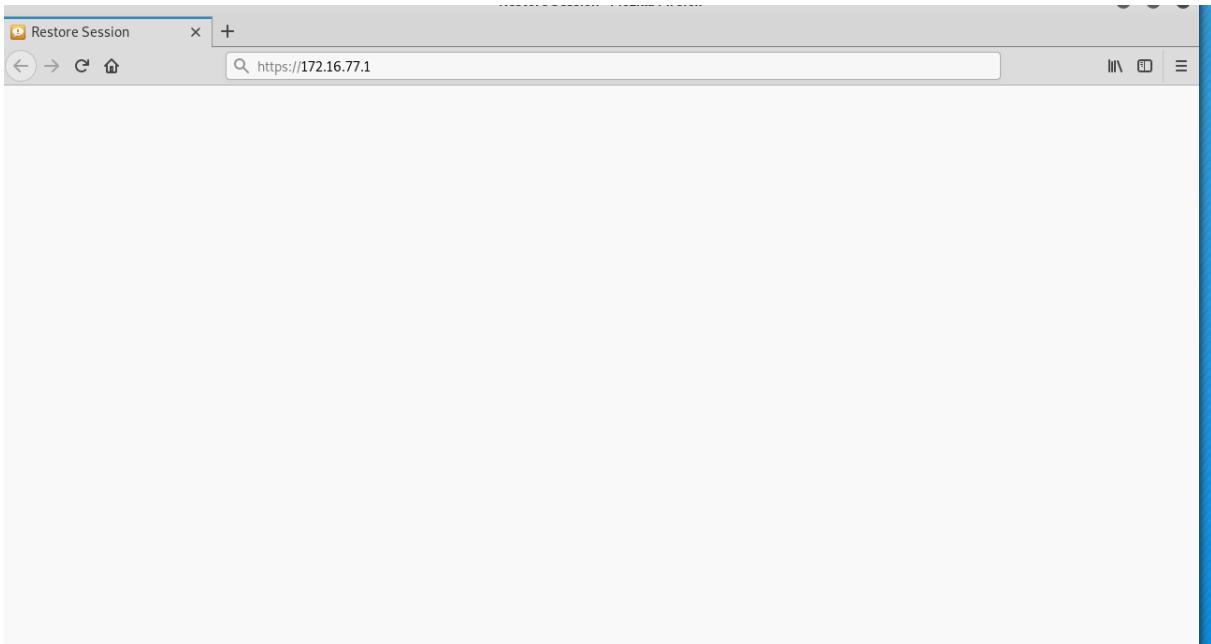
6.

```
root@kali:~# ping 192.168.1.6
PING 192.168.1.6 (192.168.1.6) 56(84) bytes of data.
64 bytes from 192.168.1.6: icmp_seq=1 ttl=64 time=0.013 ms
64 bytes from 192.168.1.6: icmp_seq=2 ttl=64 time=0.023 ms
64 bytes from 192.168.1.6: icmp_seq=3 ttl=64 time=0.023 ms
64 bytes from 192.168.1.6: icmp_seq=4 ttl=64 time=0.020 ms
^C
--- 192.168.1.6 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3077ms
rtt min/avg/max/mdev = 0.013/0.019/0.023/0.004 ms
root@kali:~# ping 172.16.77.2
PING 172.16.77.2 (172.16.77.2) 56(84) bytes of data.
^C
--- 172.16.77.2 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2048ms

root@kali:~# ping 172.16.77.3
PING 172.16.77.3 (172.16.77.3) 56(84) bytes of data.
^C
--- 172.16.77.3 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1017ms

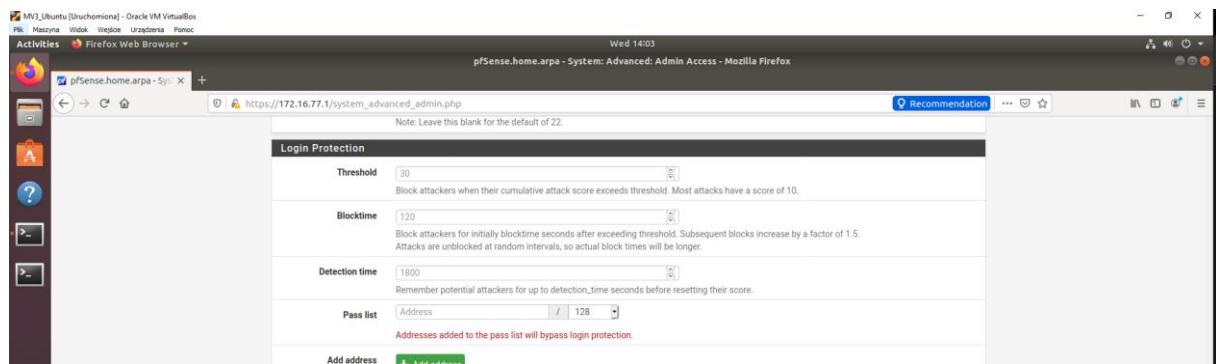
root@kali:~#
```

7.

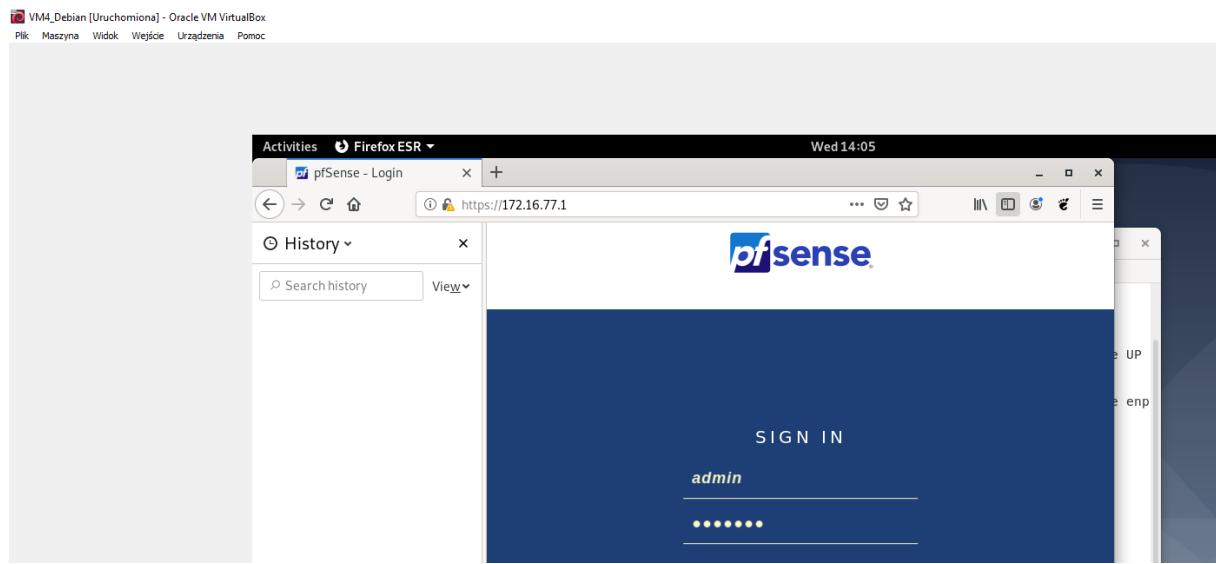


8.

Ubuntu:



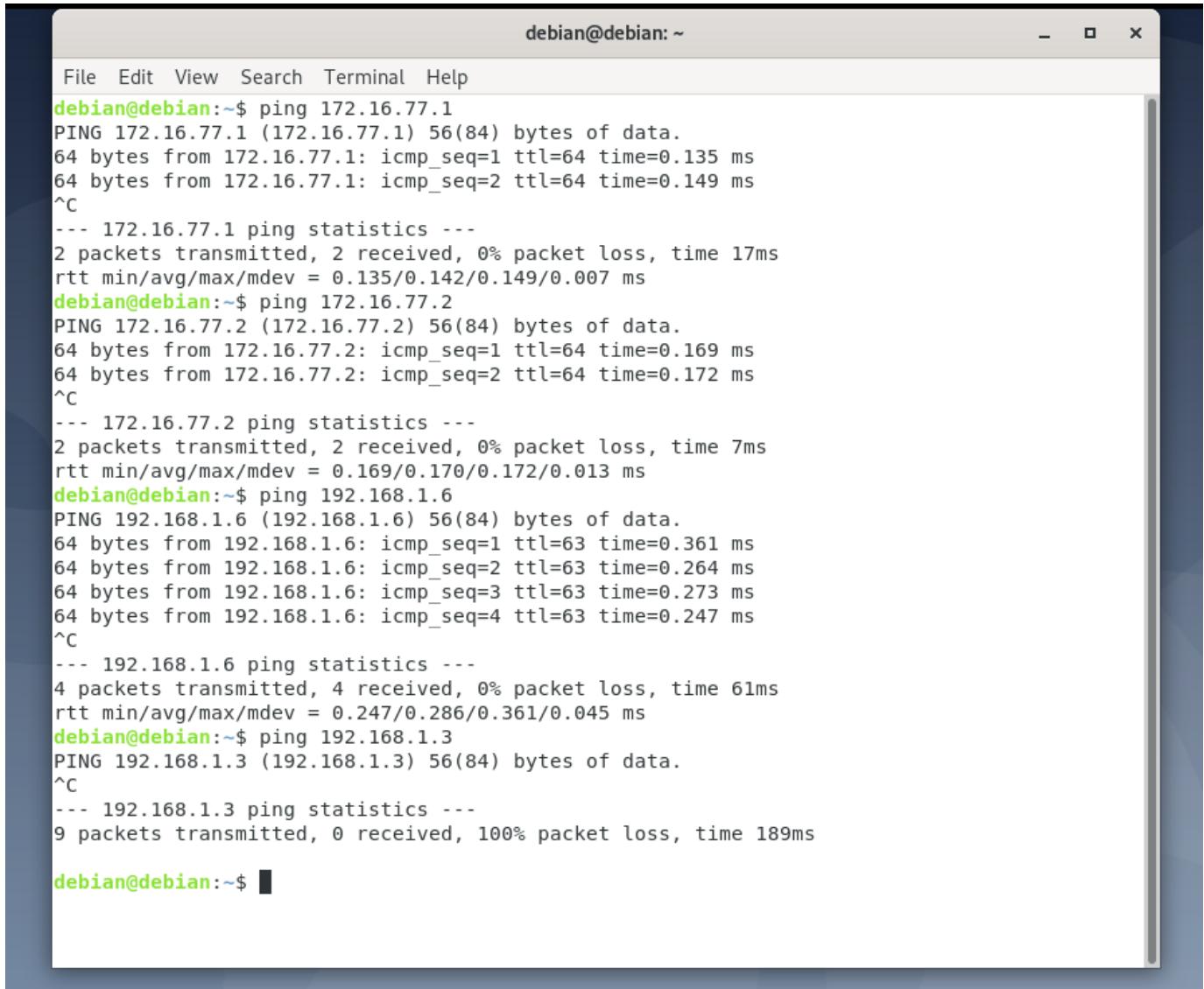
Debian:



Project Task1:

1.

a)

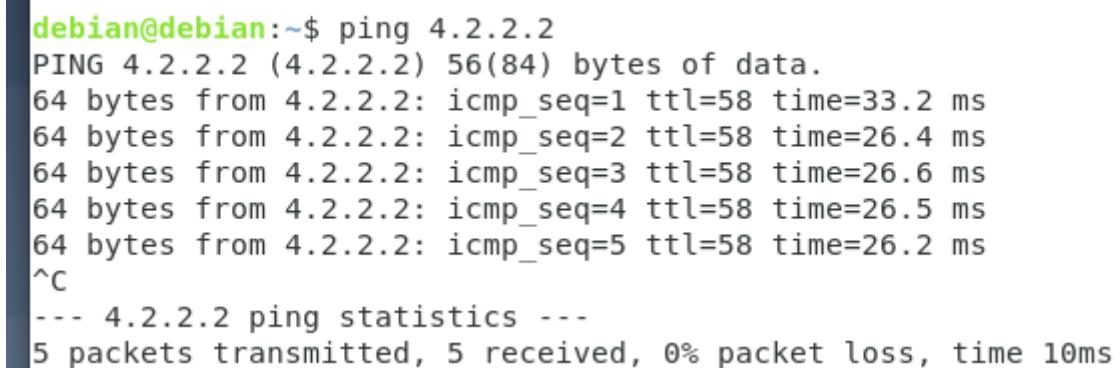


debian@debian:~

```
File Edit View Search Terminal Help
debian@debian:~$ ping 172.16.77.1
PING 172.16.77.1 (172.16.77.1) 56(84) bytes of data.
64 bytes from 172.16.77.1: icmp_seq=1 ttl=64 time=0.135 ms
64 bytes from 172.16.77.1: icmp_seq=2 ttl=64 time=0.149 ms
^C
--- 172.16.77.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 17ms
rtt min/avg/max/mdev = 0.135/0.142/0.149/0.007 ms
debian@debian:~$ ping 172.16.77.2
PING 172.16.77.2 (172.16.77.2) 56(84) bytes of data.
64 bytes from 172.16.77.2: icmp_seq=1 ttl=64 time=0.169 ms
64 bytes from 172.16.77.2: icmp_seq=2 ttl=64 time=0.172 ms
^C
--- 172.16.77.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 0.169/0.170/0.172/0.013 ms
debian@debian:~$ ping 192.168.1.6
PING 192.168.1.6 (192.168.1.6) 56(84) bytes of data.
64 bytes from 192.168.1.6: icmp_seq=1 ttl=63 time=0.361 ms
64 bytes from 192.168.1.6: icmp_seq=2 ttl=63 time=0.264 ms
64 bytes from 192.168.1.6: icmp_seq=3 ttl=63 time=0.273 ms
64 bytes from 192.168.1.6: icmp_seq=4 ttl=63 time=0.247 ms
^C
--- 192.168.1.6 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 61ms
rtt min/avg/max/mdev = 0.247/0.286/0.361/0.045 ms
debian@debian:~$ ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
^C
--- 192.168.1.3 ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 189ms

debian@debian:~$
```

b)



```
debian@debian:~$ ping 4.2.2.2
PING 4.2.2.2 (4.2.2.2) 56(84) bytes of data.
64 bytes from 4.2.2.2: icmp_seq=1 ttl=58 time=33.2 ms
64 bytes from 4.2.2.2: icmp_seq=2 ttl=58 time=26.4 ms
64 bytes from 4.2.2.2: icmp_seq=3 ttl=58 time=26.6 ms
64 bytes from 4.2.2.2: icmp_seq=4 ttl=58 time=26.5 ms
64 bytes from 4.2.2.2: icmp_seq=5 ttl=58 time=26.2 ms
^C
--- 4.2.2.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 10ms
```

c)

```

rssi mbit/avg/max/mdev = -20.185/-1.09/33.195/-1.19 ms
debian@debian:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=4.39 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=4.38 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=4.05 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 4.049/4.271/4.387/0.157 ms
debian@debian:~$ █

```

2.

The screenshot shows a Firefox browser window with the title "pfSense.home.arpa - Interfaces: WAN (em0) - Mozilla Firefox". The address bar shows the URL <https://172.16.77.1/interfaces.php?if=wlan>. The page content is a configuration form for the WAN interface. It includes fields for "DHCPv6 Prefix Delegation size" (set to 64), "Send IPv6 prefix hint" (unchecked), "Debug" (unchecked), and "Do not wait for a RA" (unchecked). Under "Do not allow PD/Address release", there is a note about dhcp6c sending a release to the ISP. The "Reserved Networks" section contains two entries: "Block private networks and loopback addresses" (unchecked) and "Block bogon networks" (checked). A note below the second entry explains that it blocks traffic from reserved IP addresses (not RFC 1918) or IANA Bogons. A "Save" button is at the bottom of the form.

3.

77.1/firewall_rules_edit.php?if=lan&after=-1

Edit Firewall Rule

Action: Block
 Choose what to do with packets that match the criteria specified below.
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: Disable this rule
 Set this option to disable this rule without removing it from the list.

Interface: LAN
 Choose the interface from which packets must come to match this rule.

Address Family: IPv4
 Select the Internet Protocol version this rule applies to.

Protocol: ICMP
 Choose which IP protocol this rule should match.

ICMP Subtypes: Router solicitation, SKIP, Source quench, Timestamp reply
 For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Source
 Source: Invert match, any, Source Address /

Destination
 Destination: Invert match, Single host or alias, 8.8.8.8 /

Extra Options
 Log: Log packets that are handled by this rule
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
 Description:
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
 Advanced Options:

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 /315 KIB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0 /0 B	IPv4 ICMP any	*	*	8.8.8.8	*	*	none			
<input type="checkbox"/>	✓ 2 /10.59 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Save

4.

```

    / packets transmitted, / received, 0% packet loss, time 0:149ms
    rtt min/avg/max/mdev = 0.156/0.188/0.259/0.043 ms
ubuntu@ubuntu-VirtualBox:~$ ping 4.2.2.2
PING 4.2.2.2 (4.2.2.2) 56(84) bytes of data.
64 bytes from 4.2.2.2: icmp_seq=1 ttl=58 time=26.3 ms
64 bytes from 4.2.2.2: icmp_seq=2 ttl=58 time=26.0 ms
64 bytes from 4.2.2.2: icmp_seq=3 ttl=58 time=26.2 ms
^C
--- 4.2.2.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 26.043/26.227/26.353/0.229 ms
ubuntu@ubuntu-VirtualBox:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.

```

System Firewall DHCP Authentication IPsec PPP PPPoE/L2TP Server OpenVPN NTP Packages Settings

Normal View Dynamic View Summary View

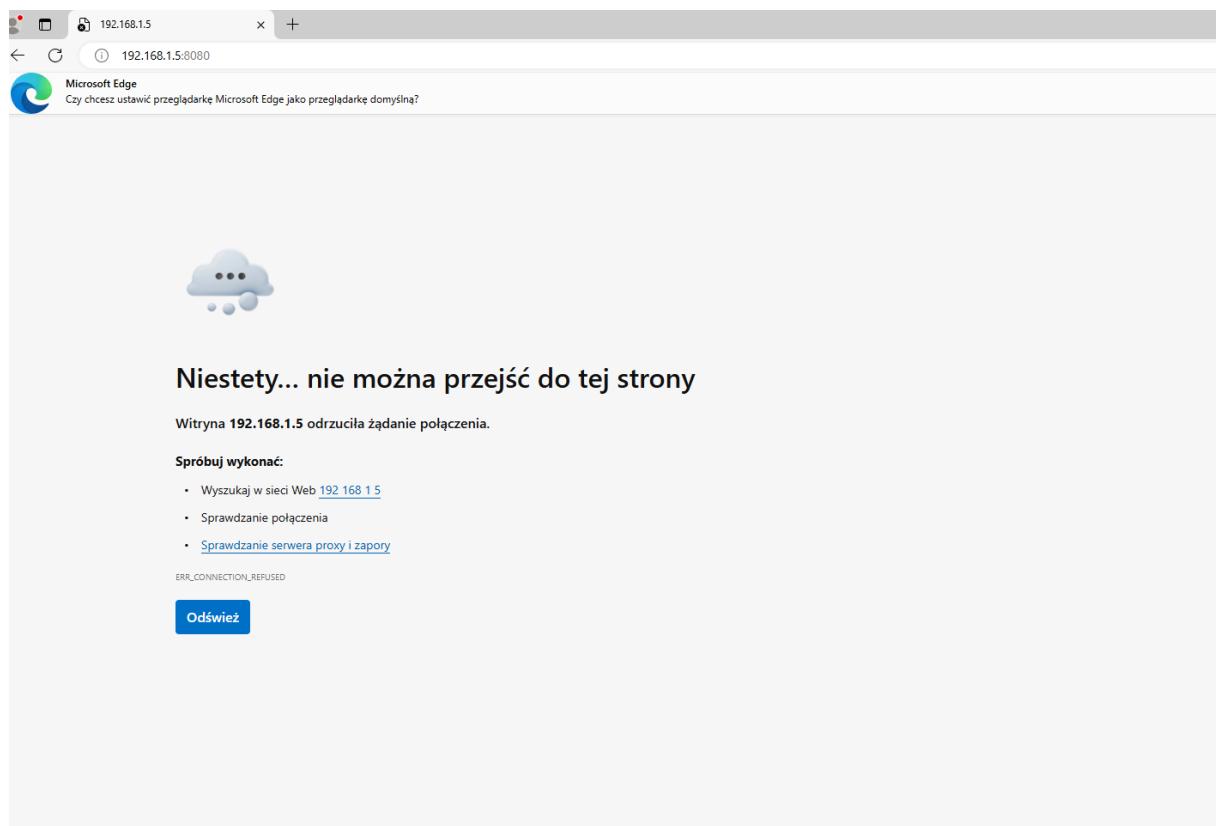
Last 231 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Aug 7 20:19:03	LAN	USER_RULE (1723061880)	172.16.77.2	8.8.8.8	ICMP
✗	Aug 7 20:19:04	LAN	USER_RULE (1723061880)	172.16.77.2	8.8.8.8	ICMP
✗	Aug 7 20:19:05	LAN	USER_RULE (1723061880)	172.16.77.2	8.8.8.8	ICMP
✗	Aug 7 20:19:06	LAN	USER_RULE (1723061880)	172.16.77.2	8.8.8.8	ICMP
✗	Aug 7 20:19:07	LAN	USER_RULE (1723061880)	172.16.77.2	8.8.8.8	ICMP
✗	Aug 7 20:19:08	LAN	USER_RULE (1723061880)	172.16.77.2	8.8.8.8	ICMP
✗	Aug 7 20:19:09	LAN	USER_RULE (1723061880)	172.16.77.2	8.8.8.8	ICMP
✗	Aug 7 20:19:10	LAN	USER_RULE (1723061880)	172.16.77.2	8.8.8.8	ICMP
✗	Aug 7 20:19:11	LAN	USER_RULE (1723061880)	172.16.77.2	8.8.8.8	ICMP
✗	Aug 7 20:19:12	LAN	USER_RULE (1723061880)	172.16.77.2	8.8.8.8	ICMP
✗	Aug 7 20:19:13	LAN	USER_RULE (1723061880)	172.16.77.2	8.8.8.8	ICMP
✗	Aug 7 20:19:14	LAN	USER_RULE (1723061880)	172.16.77.2	8.8.8.8	ICMP
✗	Aug 7 20:19:16	LAN	USER_RULE (1723061880)	172.16.77.2	8.8.8.8	ICMP
✗	Aug 7 20:19:17	LAN	USER_RULE (1723061880)	172.16.77.2	8.8.8.8	ICMP
✗	Aug 7 20:19:18	LAN	USER_RULE (1723061880)	172.16.77.2	8.8.8.8	ICMP
✗	Aug 7 20:19:19	LAN	USER_RULE (1723061880)	172.16.77.2	8.8.8.8	ICMP

Project Task2:

1.

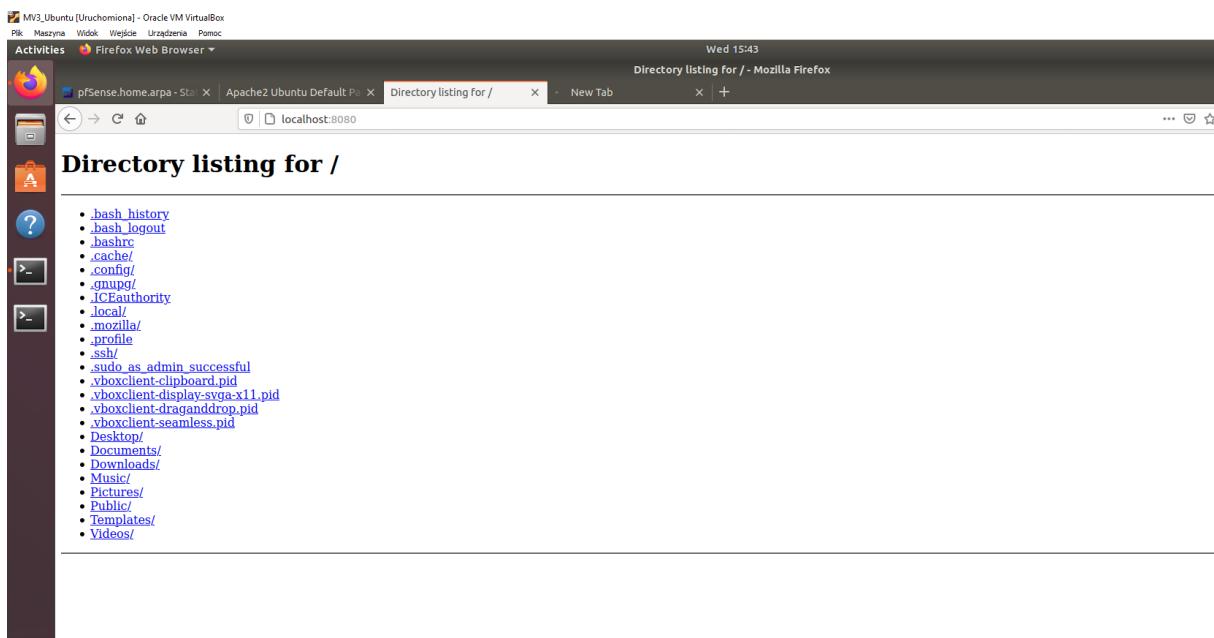
```
ubuntu@ubuntu-VirtualBox:~$ sudo python3 -m http.server 8080
[sudo] password for ubuntu:
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
172.16.77.2 - - [07/Aug/2024 15:13:15] "GET / HTTP/1.1" 200 -
172.16.77.2 - - [07/Aug/2024 15:13:15] code 404, message File not found
172.16.77.2 - - [07/Aug/2024 15:13:15] "GET /favicon.ico HTTP/1.1" 404 -
172.16.77.2 - - [07/Aug/2024 15:13:30] "GET / HTTP/1.1" 200 -
172.16.77.2 - - [07/Aug/2024 15:13:30] code 404, message File not found
172.16.77.2 - - [07/Aug/2024 15:13:30] "GET /favicon.ico HTTP/1.1" 404 -
```



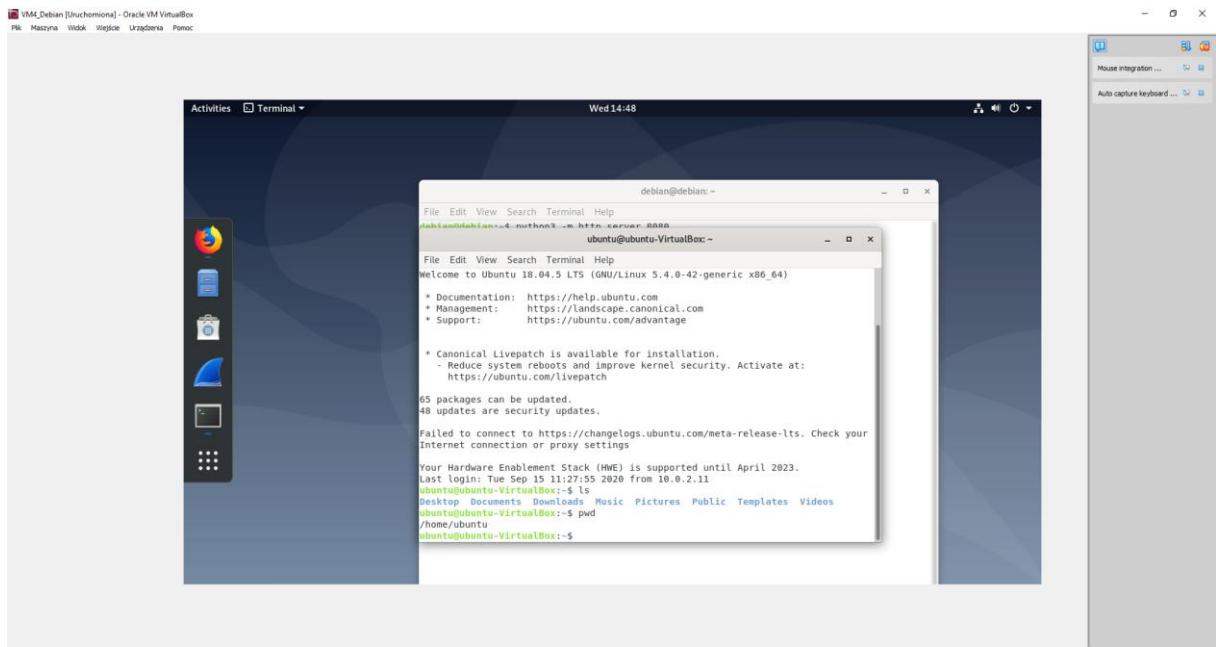
What is the issue in accessing the web server from your host machine?

NAT nie został skonfigurowany

2.



3.



4.

SSH

Edit Redirect Entry

Disabled	<input type="checkbox"/> Disable this rule			
No RDR (NOT)	<input type="checkbox"/> Disable redirection for traffic matching this rule This option is rarely needed. Don't use this without thorough knowledge of the implications.			
Interface	WAN			
Choose which interface this rule applies to. In most cases "WAN" is specified.				
Address Family	IPv4			
Select the Internet Protocol version this rule applies to.				
Protocol	TCP/UDP			
Choose which protocol this rule should match. In most cases "TCP" is specified.				
Source	Display Advanced			
Destination	<input type="checkbox"/> Invert match.	WAN address	/	Address/mask
Destination port range	SSH	Custom	SSH	Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.				
Redirect target IP	Single host	172.16.77.2		
Type	Address			
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4 In case of IPv6 addresses, it must be from the same "scope". i.e. it is not possible to redirect from link-local addresses scope (fe80::) to local scope (::1)				
Redirect target port	SSH	Custom		
Port	Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).			
This is usually identical to the "From port" above.				
Description	SSH			
A description may be entered here for administrative reference (not parsed).				
No XMLRPC Sync	<input type="checkbox"/> Do not automatically sync to other CARP members			
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.				
NAT reflection	Use system default			
Filter rule association	Rule NAT SSH			
View the filter rule				

Rule Information

Created	8/7/24 21:36:46 by admin@172.16.77.2 (Local Database)
Updated	8/7/24 21:36:46 by admin@172.16.77.2 (Local Database)

[Save](#)

http

Edit Redirect Entry

Disabled	<input type="checkbox"/> Disable this rule
No RDR (NOT)	<input type="checkbox"/> Disable redirection for traffic matching this rule This option is rarely needed. Don't use this without thorough knowledge of the implications.
Interface	WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.	
Address Family	IPv4
Select the Internet Protocol version this rule applies to.	
Protocol	TCP/UDP
Choose which protocol this rule should match. In most cases "TCP" is specified.	
Source	Display Advanced
Destination	<input type="checkbox"/> Invert match. Type: WAN address / Address/mask
Destination port range	Other: 8080 From port: Custom To port: 8080 To port: Custom Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.
Redirect target IP	Type: Single host Address: 172.16.77.2 <small>Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4 In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80::*) to local scope (::1)</small>
Redirect target port	Port: 8080 <small>Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically). This is usually identical to the "From port" above.</small>
Description	HTTP
A description may be entered here for administrative reference (not parsed).	
No XMLRPC Sync	<input type="checkbox"/> Do not automatically sync to other CARP members This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.
NAT reflection	Use system default
Filter rule association	Rule NAT HTTP
View the filter rule	
Rule Information	
Created	8/7/24 21:35:37 by admin@172.16.77.2 (Local Database)
Updated	8/7/24 21:35:37 by admin@172.16.77.2 (Local Database)
<input type="button" value="Save"/>	

Port Forward 1:1 Outbound NPt

Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	22 (SSH)	172.16.77.2	22 (SSH)	SSH	Edit Delete
<input type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	8080	172.16.77.2	8080	HTTP	Edit Delete

Legend

Firewall / Rules / WAN

Floating WAN LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0 / 4 KiB	IPv4 TCP/UDP	*	*	172.16.77.2	8080	*	none	NAT HTTP		
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP/UDP	*	*	172.16.77.2	22 (SSH)	*	none	NAT SSH		

Add Add Delete Save Separator

Physical host

Directory listing for /

- bash_history
- bash_logout
- bashrc
- cache
- config
- mozilla
- ICEAuthority
- local
- mozilla/
- profile
- ssh
- .ssh_as_admin_successful
- vbclient-clipboard.pid
- vbclient-display-avra-x11.pid
- vbclient-draganddrop.pid
- vbclient-seamless.pid
- Desktop/
- Documents/
- Downloads/
- Music/
- Pictures/
- Public/
- Templates/
- Videos/

Project Task3:

1.

Usługa, która może spełnić wymagania CISO to suricata.

2.

Version	2.6.0-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE
---------	---

3.

System / Package Manager / Package Installer

pfSense-pkg-suricata installation successfully completed.

Installed Packages Available Packages Package Installer

Package Installation

Time to run in netmap(4) mode.

RULES: Suricata IDS/IPS Engine comes without rules by default. You should add rules by yourself and set an updating strategy. To do so, please visit:

<http://www.openinfosecfoundation.org/documentation/rules.html>
<http://www.openinfosecfoundation.org/documentation/emerging-threats.html>

You may want to try BPF in zerocopy mode to test performance improvements:

sysctl -w net.bpf.zerocopy_enable=1

Don't forget to add net.bpf.zerocopy_enable=1 to /etc/sysctl.conf
>> Cleaning up cache... done.
Success

4. Services / Suricata / Updates

Interfaces Global Settings Updates Alerts Blocks Files Pass Lists Suppress Logs View Logs Mgmt SID Mgmt

Sync IP Lists

INSTALLED RULE SET MD5 SIGNATURES

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Emerging Threats Open Rules	Not Downloaded	Not Downloaded
Snort Subscriber Rules	Not Enabled	Not Enabled
Snort GPLv2 Community Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled
ABUSE.ch SSL Blacklist Rules	Not Enabled	Not Enabled

UPDATE YOUR RULE SET

Last Update: Aug-08 2024 02:16
Result: failed

MANAGE RULE SET LOG

Z jakiegoś nieznanego powodu, szukając w sieci sposobu na naprawienie tego, za każdym razem, aktualizacja nie przechodzi, nie mogę wykonać ostatnich punktów.

5,6.

```
root@kali:~# hping --flood -V -p 80 192.168.1.7
bash: hping: command not found
root@kali:~# hydra -l user -P /usr/share/worldlists/rockyou.txt ssh://192.168.1.7:22
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-07 18:21:36
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[ERROR] File for passwords not found: /usr/share/worldlists/rockyou.txt
root@kali:~#
```