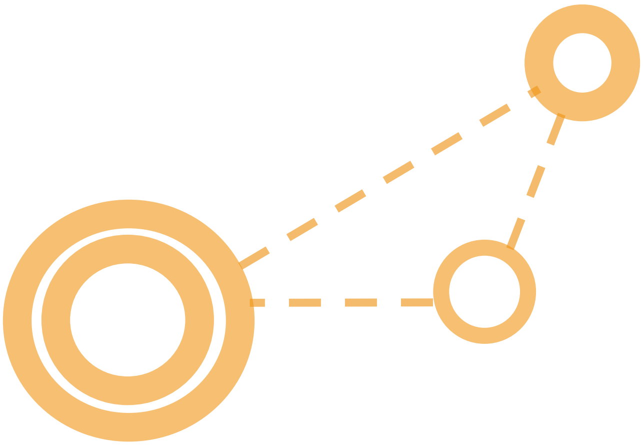
GNS3 FOR SECURITY PRACTITIONERS

A PRACTICAL GUIDE

Ana Nieto Jiménez
Javier López Muñoz



Do you want to learn more? We are teaching this and much more as part of the "Master's Degree in Computer Engineering" – Cybersecurity Experts, take a look to the program and enroll!!: https://www.uma.es/master-en-ingenieria-informatica/cms/menu/informacion-general/

If you have any comment or question about this guide, please contact with Ana Nieto, nieto@lcc.uma.es

OCTOBER 29, 2019

TABLE OF CONTENTS

LIST OF FIGURES

GOAL OF THIS GUIDE: WHAT IT IS (AND IS NOT) FOR

The objective of this guide is to provide **useful information for the development of a virtual laboratory using GNS3 with the aim of testing security features**.

This guide **is not** the container of all universal knowledge about GNS3, Kali or security tools. Use this guide as it is: an starting point for your security training.

ACRONYMS

Acronym	Meaning
AAA	Authentication, Authorization, and Accounting
API	Application Programming Interface
CDP	Cisco Discovery Protocol
C-ICAP	C-Internet Content Adaptation Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DNSBL	Domain Name System-based Blackhole List
ET	Emerging Threat
GNS3	Graphical Network Simulator-3
HIDS	Host Intrusion Detection System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
MITM	Man In The Middle
MNDP	MikroTik Neighbor Discovery Protocol
NAT	Network Address Translation
NIDS	Network Intrusion Detection System
NSE	*Nmap Scripting Engine*
OSIF	Open Information Security Foundation
OSSIM	Open Source Security Information Management
OWA	Outlook Web Access
SANS	SysAdmin, Audit, Network, Security
SIEM	Security Information and Event Management
SMB	Server Message Block
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
VLAN	Virtual LAN
VM	Virtual Machine
VPCS	Virtual PC Simulator
WAN	Wide Area Network

BOOKS

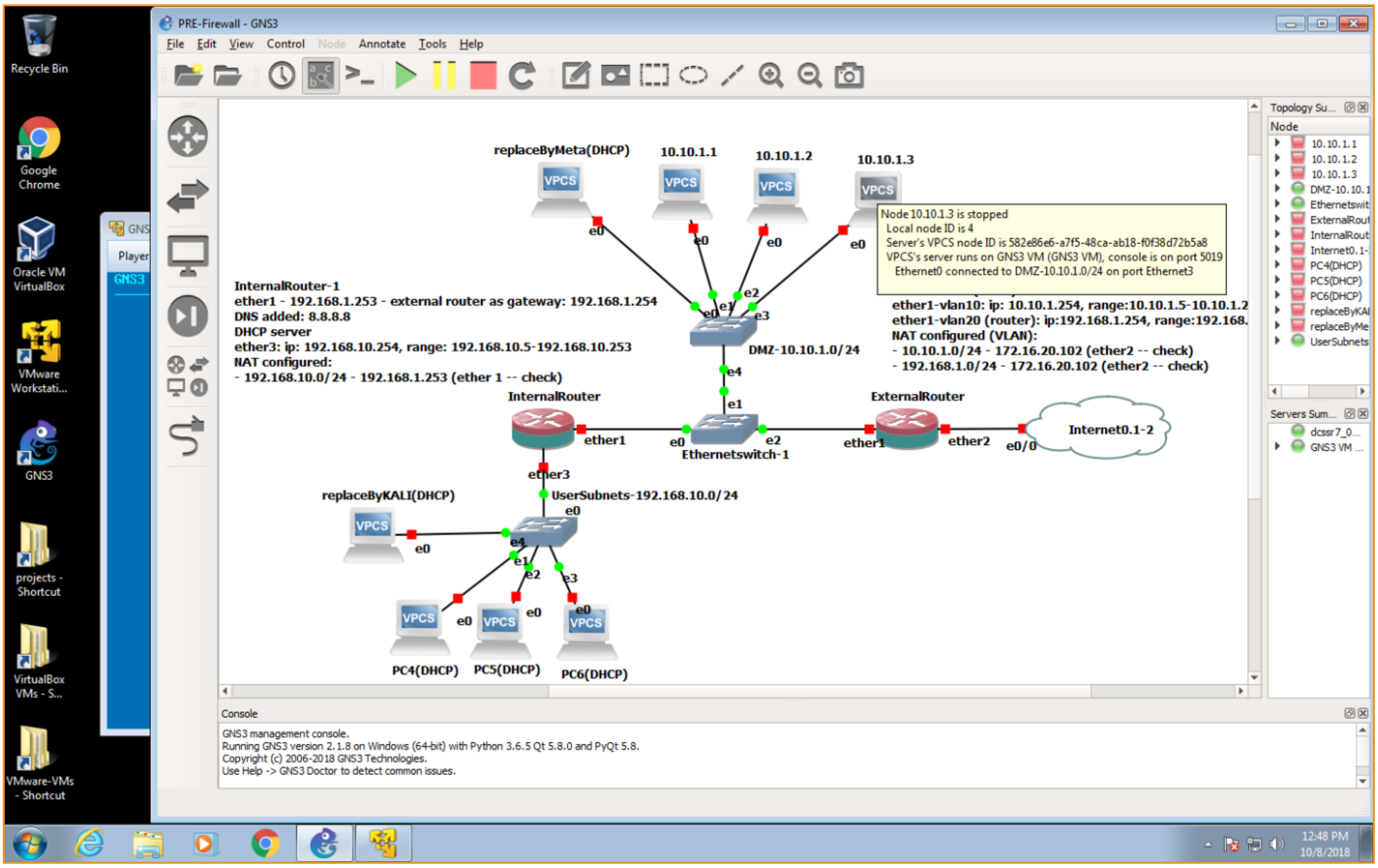
Some books of reference that can be used to complete some parts are listed below:

Reference	Book
Chris2017	Sanders, Chris. *Practical packet analysis: Using Wireshark to solve real-world network problems*. No Starch Press, 2017.
Dieterle2016	Dieterle, Daniel W. *Basic Security Testing with Kali Linux*. 2016. ISBN:978-1530506569
Dieterle2015	Dieterle, Daniel W. Intermediate security testing with kali linux 2. 2015. ISBN: 978-1516945863
Halton2016	Halton, Wolf, and Bo Weaver. *Kali Linux 2: Windows Penetration Testing*. Packt Publishing Ltd, 2016.
Hutchens2014	Hutchens, Justin. *Kali Linux network scanning cookbook*. Packt Publishing Ltd, 2014.

1 GENERAL REMARKS

In this guide GNS3 is used together with other tools for training in network security. It is possible to install all these tools in a single virtual machine. In this case, please consider that the resulting virtual machine can require 10GB of memory and can take about 100GB of disk space. In addition, the virtual machine must have nested virtualisation enabled in order to run inside other virtual machines. This is needed in order to perform security tests using the following virtual machines (included in the virtual machine core), that will be used from GNS3:

Virtual Machine Name	Description
Kali Linux 2018	Penetration testing virtual machine. This is used to find vulnerabilities and launch attacks in our network. **VMware.**
Metasploitable 3	Windows Server 2008 with vulnerabilities. Rapid 7. **VirtualBox.**
Metasploitable 2	Linux with vulnerabilities. Rapid 7. **VMware.**
HoneyDrive	Virtual machine with honehypots.



InternalRouter-1
ether1 - 192.168.1.253 - external router as gateway: 192.168.1.254
DNS added: 8.8.8.8
DHCP server
ether3: ip: 192.168.10.254, range: 192.168.10.5-192.168.10.253
NAT configured:
- 192.168.10.0/24 - 192.168.1.253 (ether 1 -- check)

Node 10.10.1.3 is stopped
Local node ID is 4
Server's VPCS node ID is 582e86e6-a7f5-48ca-ab18-f0f38d72b5a8
VPCS's server runs on GNS3 VM (GNS3 VM), console is on port 5019
Ethernet0 connected to DMZ-10.10.1.0/24 on port Ethernet3

ether1-vlan10: ip: 10.10.1.254, range:10.10.1.5-10.10.1.2
ether1-vlan20 (router): ip:192.168.1.254, range:192.168.
NAT configured (VLAN):
- 10.10.1.0/24 - 172.16.20.102 (ether2 -- check)
- 192.168.1.0/24 - 172.16.20.102 (ether2 -- check)

```
GNS3 management console.
Running GNS3 version 2.1.8 on Windows (64-bit) with Python 3.6.5 Qt 5.8.0 and PyQt 5.8.
Copyright (c) 2006-2018 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.
```

Figure 1. Virtual machine prepared with GNS3

The following sections describe the basics about GNS3 and how this can be installed in a platform for our purposes.

2 GNS3

GNS3 is a complete network simulation environment with the peculiarity that allows us to include ***virtual machines*** in order to test different scenarios, using different network architectures (https://gns3.com/software).

Note that, as any other tool, GNS3 also has limitations, for example, it cannot be used to test wireless scenarios. If the student requires to test alternative scenarios, he/she can use PacketTracer.

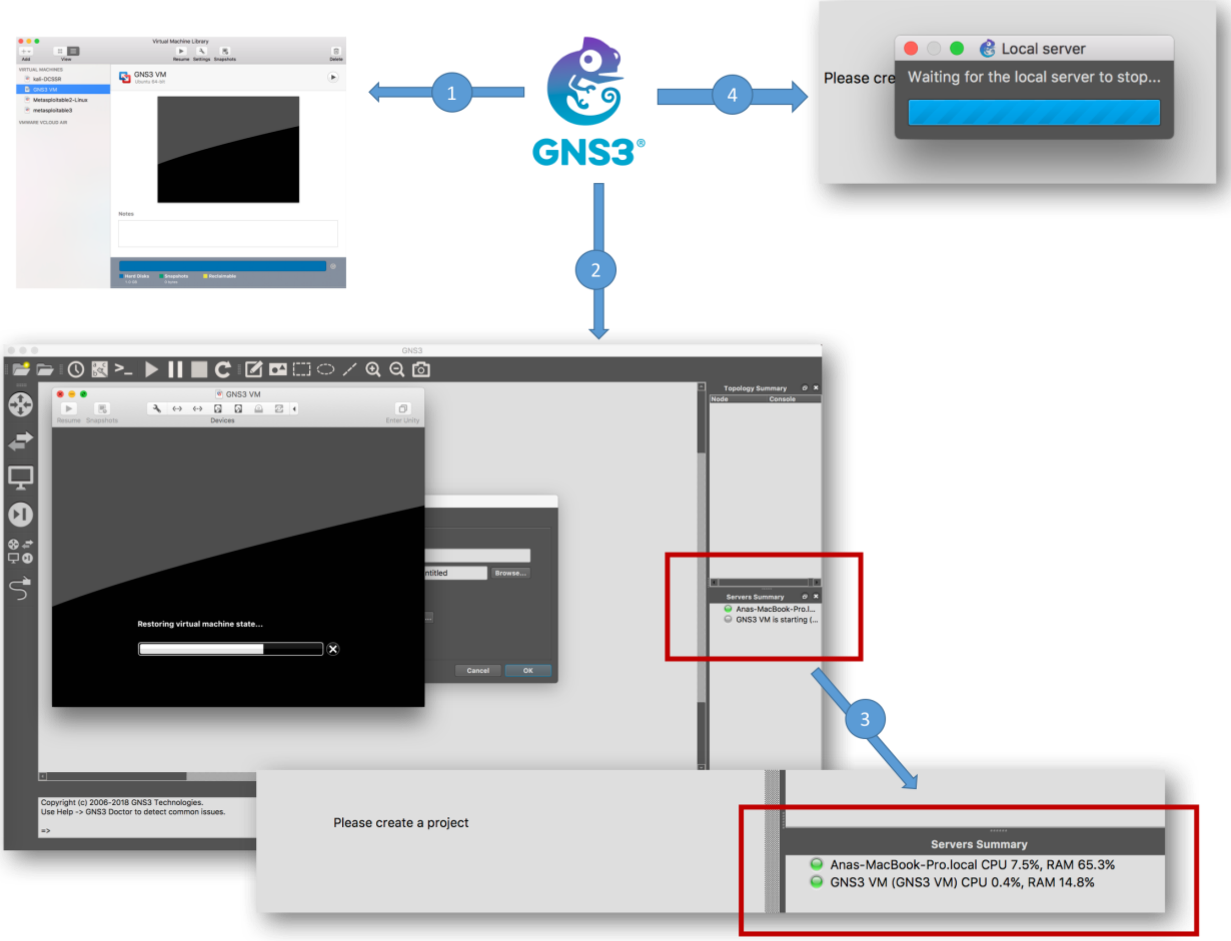
2.1 BASICS ABOUT GNS3

First, is important to be familiarised with the basic concepts about how GNS3 works.

The following phases refer to the figure below:

1. GNS3 will invoke VMware player in order to launch automatically GNS3 VM, that is a special virtual machine.
2. If everything is fine, then the application automatically opens and handles GNS3 VM (you need to do nothing). GNS3 VM is our additional server to emulate the rest of devices.
3. The student can see that there are two servers: the server with name "GNS3 VM" is the virtual machine, and the additional server is a service allocated on the student's machine (host).

   NOTE: Please do not interact with GNS3 VM unless the professor tells you to do it.
4. When the student decides to close GNS3, the application will automatically power off the virtual machine (and all the devices and additional VM) and the rest of servers.



Local server

Please cre

Waiting for the local server to stop...

Restoring virtual machine state...

Servers Summary

Anas-MacBook-Pro.l...

GNS3 VM is starting (...

Copyright (c) 2006-2018 GNS3 Technologies.
Use Help -> GNS3 Doctor to detect common issues.

Please create a project

Servers Summary

Anas-MacBook-Pro.local CPU 7.5%, RAM 65.3%

GNS3 VM (GNS3 VM) CPU 0.4%, RAM 14.8%

Figure 2. Basics GNS3

It must be noted that, at home, the student may use GNS3 without GNS3 VM, though it is strongly recommended to use it. Some components (e.g. Cisco routers) depends on GNS3 VM.

2.2 RECOMMENDED VIRTUAL PLATFORM

If the student does not have a license for VMWare, it is recommended to download **VMware Workstation Player 12** (not 14). The student just need to provide an own e-mail address in order to use this version of VMWare to work with virtual machines. It is also necessary to install **VIX API**. This is required in order for GNS3 to be able to launch virtual machines.

It is critical to respect the **default directory chosen by VMware Workstation Player for allocation of VMs** (**C:\Users\alumno\Documents\Virtual Machines**).

The student can choose to use VirtualBox, though in that case it should bear in mind that its use is different from VMware and that this Guide will not be helpful.

It must be further noted that VirtualBox will be used to launch Metasploitable 3. But this is only an exception. In general, VMware will be the preferred platform.

2.3 INSTALLATION

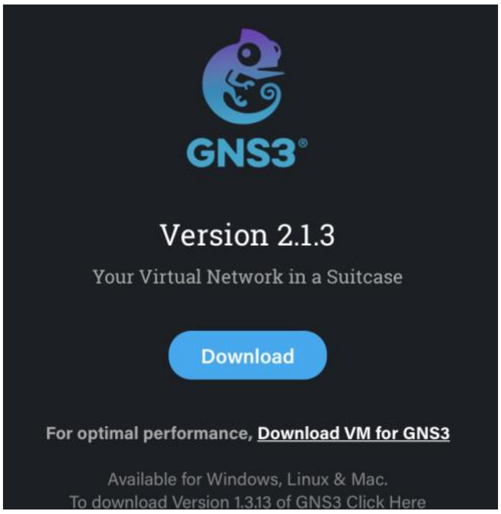
In order to install GNS3, it is necessary to download the software from the official page after registration.

The student must download:

- The software for GNS3 (blue button in the picture) and
- The virtual machine for GNS3 (see link at bottom of the picture)

Important:

- It is necessary to download the virtual machine for GNS3 (GNS3 VM) according to your virtual platform.
- And, also, to **import the GNS3 VM in the Virtual Machine Library before opening GNS3.**



Version 2.1.3

Your Virtual Network in a Suitcase

For optimal performance, Download VM for GNS3

Available for Windows, Linux & Mac.

To download Version 1.3.13 of GNS3 Click Here

Figure 3. GNS3 download

2.3.1 GNS3 VM

The student also needs the GNS3 Virtual Machine in order to improve the performance of GNS3 application. In general, GNS3 VM will not be used directly; it will be used by GNS3 to emulate the network devices.

2.3.1.1 KEYBOARD

To change to Spanish keyboard, use **loadkeys es**. If it does not work, use “sudo”. Alternatively, note that the upper case + “ñ” is equal to “:”, and “-“ is equal to “/”.

2.4 FIRST TEST: CONFIGURE A BASIC VIRTUAL NETWORK

In this section, we are going to connect two virtual PCs using an Ethernet switch. When including new virtual elements, the student has to select GNS3 VM. Next picture shows two options: one is for the local server, and the second one (selected) is for GNS3 VM.

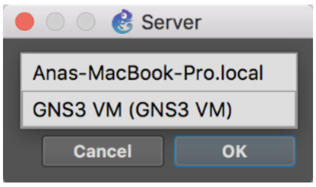


Figure 4. Selection of the server to run the virtual elements

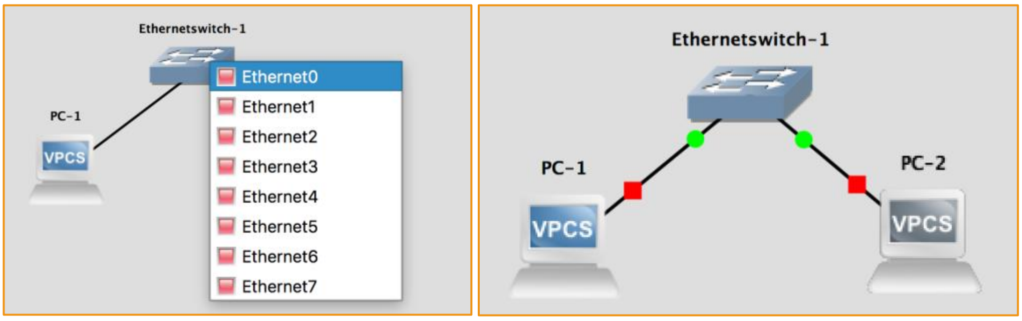
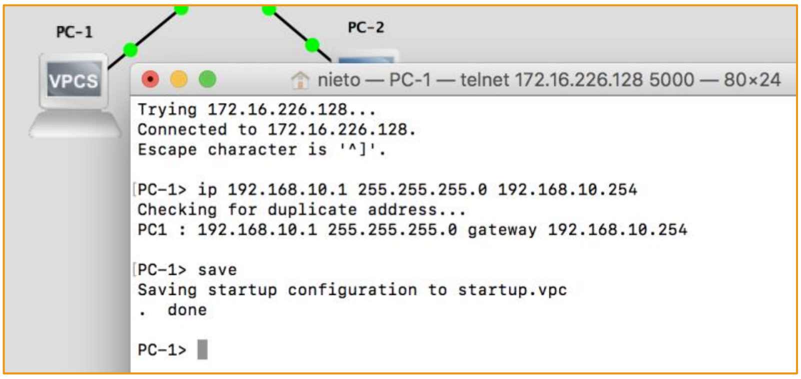


Figure 5. Two virtual PCs (VPCS) connected

The red square means that the VPCS are shut down. By using the green triangle (play symbol) it is possible to power on all the network elements.

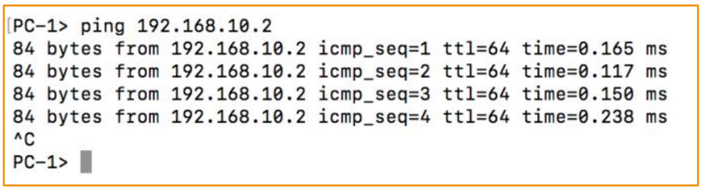


```
Trying 172.16.226.128...
Connected to 172.16.226.128.
Escape character is '^]'.

PC-1> ip 192.168.10.1 255.255.255.0 192.168.10.254
Checking for duplicate address...
PC1 : 192.168.10.1 255.255.255.0 gateway 192.168.10.254

PC-1> save
Saving startup configuration to startup.vpc
.  done

PC-1>
```

Figure 6. IP configuration

Configure the IP for each VPCS using the option “Console” (right button on the network element). Ip <ip-address> <ipmask> <gateway-ip>. In this initial configuration a gateway is not used, but it is equally indicated in order to prepare the scenario to future use cases.

Once the VPCS are configured, it should be possible to execute ***ping*** from each other, as shown in the following picture.



```
PC-1> ping 192.168.10.2
84 bytes from 192.168.10.2 icmp_seq=1 ttl=64 time=0.165 ms
84 bytes from 192.168.10.2 icmp_seq=2 ttl=64 time=0.117 ms
84 bytes from 192.168.10.2 icmp_seq=3 ttl=64 time=0.150 ms
84 bytes from 192.168.10.2 icmp_seq=4 ttl=64 time=0.238 ms
^C
PC-1>
```

Figure 7. Effective ping from PC-1 (192.168.10.1) to PC-2 (192.168.10.2)

2.5 SECOND TEST: CONFIGURE A VIRTUAL MACHINE FOR GNS3: KALI LINUX AS USE CASE

The following steps would be needed to configure the Kali Linux virtual machine in GNS3, during the sessions in the laboratory.

2.5.1 VMWARE WORKSTATION PLAYER AND OUR VIRTUAL MACHINES

First, check that the virtual machine is listed in **Virtual Machine Library**, and that this is allocated in the default path for VMs of VMWare Workstation Player. The virtual machine library can be seen when opening VMWare Workstation Player. The virtual machine must be shut down.

2.5.2 CREATE A TEMPLATE FOR GNS3

Edit/Preferences

Select **VMware VMs** as next picture shows:

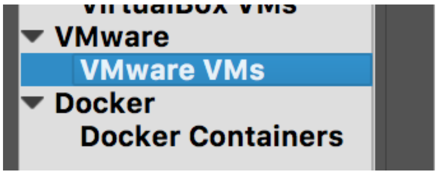
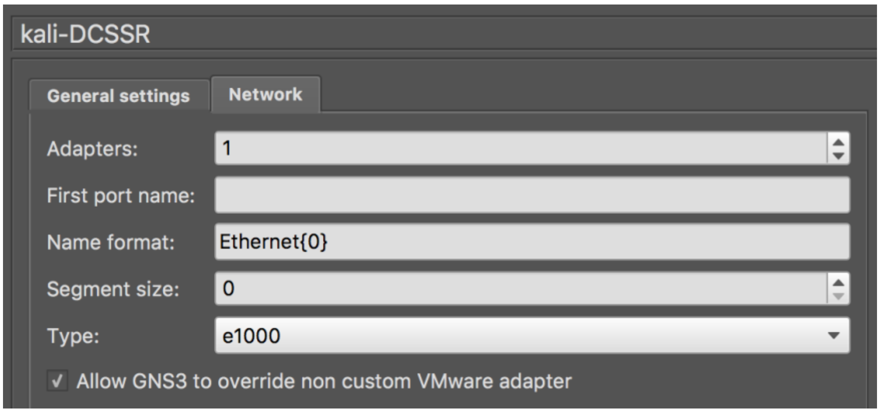


Figure 8. VMware VMs option in Edit/Preferences (Windows) or GNS3/Preferences (Mac OS)

New is for adding a new template. Default option: "Run this VMware VM on my local computer". In the next window, you have to select the **Kali Linux VM** in the **VM list**. If the virtual machine is not in the list, please check that it is listed in the **Virtual Machine Library**. Finish.

Then, it is necessary to edit the virtual machine, and select the option "Allow GNS3 to override non custom VMware adapter".


kali-DCSSR

General settings | Network

Adapters: 1

First port name:

Name format: Ethernet{0}

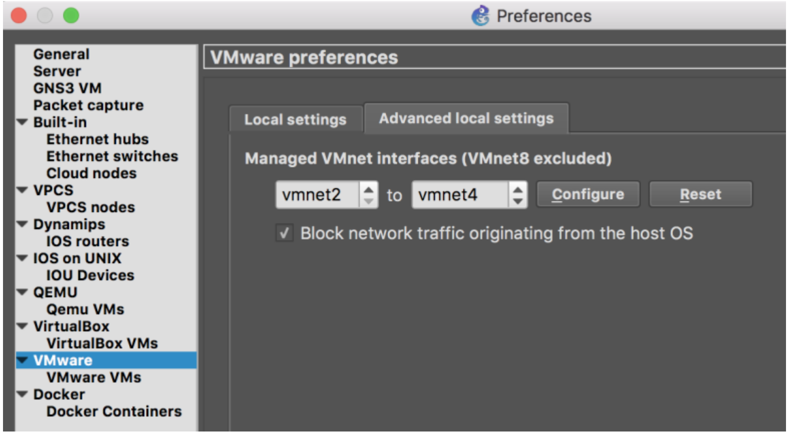
Segment size: 0

Type: e1000

☑ Allow GNS3 to override non custom VMware adapter

Figure 9. Virtual Machine template for Kali-DCSSR VM

Finally, it is necessary to create the VMware interfaces. This can be done in the option VMware (Preferences), in "Advanced local settings", with the button "Configure". Note that we only create 3 interfaces.



Managed VMnet interfaces (VMnet8 excluded)

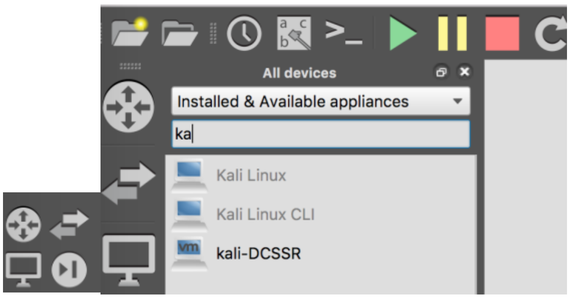
vmnet2 to vmnet4

☑ Block network traffic originating from the host OS

Figure 10. Configure VMnet interfaces

2.5.3 SELECT YOUR TEMPLATE

The student can see the template in the list of available templates, as the next picture shows. Then, select the template and put it in the workspace.



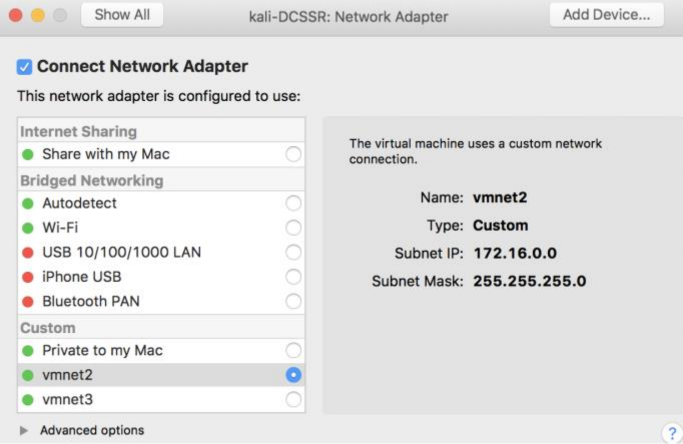
ka

- Kali Linux
- Kali Linux CLI
- kali-DCSSR

Figure 11. Search your template

2.5.4 SET UP THE NETWORK ADAPTER IN VMWARE PLAYER FOR THE VIRTUAL MACHINE

Finally, it is necessary to select the network adapter for the virtual machine in VMware Player, as shown next:



☑ Connect Network Adapter

This network adapter is configured to use:

Internet Sharing
- Share with my Mac ○

Bridged Networking
- Autodetect ○
- Wi-Fi ○
- USB 10/100/1000 LAN ○
- iPhone USB ○
- Bluetooth PAN ○

Custom
- Private to my Mac ○
- vmnet2 ●
- vmnet3 ○

The virtual machine uses a custom network connection.

Name:	vmnet2
Type:	Custom
Subnet IP:	172.16.0.0
Subnet Mask:	255.255.255.0

Figure 12. Select network adapter for the virtual machine

The picture corresponds to VMware Fusion, but the option is quite similar in VMware Workstation Player.

2.5.5 CONFIGURE THE NETWORK ADAPTER OF THE VIRTUAL MACHINE

Start the virtual machine from GNS3, as shown:

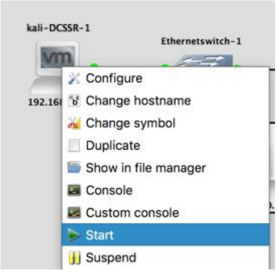
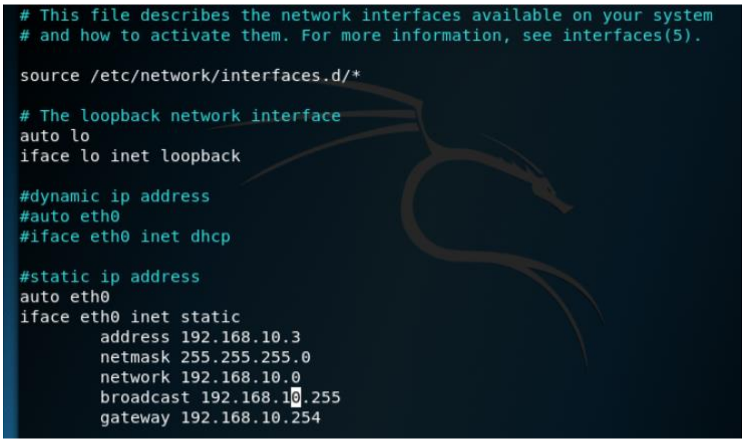


Figure 13. Start a network element

Then, GNS3 will open the virtual machine using VMware player. You can configure the virtual machine using VMware player. Initiate session in the Kali using the user: **root**, and the password: **toor**.

2.5.5.1 Static IP

In order to configure a static IP in *eth0*, edit */etc/network/interfaces* and add the text that appears in the next figure. Note that, in the same figure, it is possible to observe the options for dynamic IP (DHCP) commented with #.



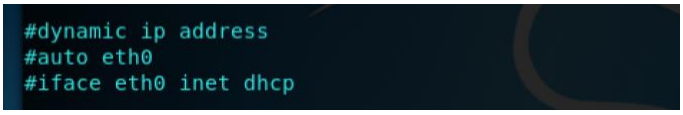
```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

#dynamic ip address
#auto eth0
#iface eth0 inet dhcp

#static ip address
auto eth0
iface eth0 inet static
        address 192.168.10.3
        netmask 255.255.255.0
        network 192.168.10.0
        broadcast 192.168.10.255
        gateway 192.168.10.254
```

Figure 14. Static IP

To set up the changes, save the changes in the file, exit and use the commands: **ifdown eth0** followed by **ifup eth0**.

2.5.5.2 Dynamic IP

To configure a dynamic IP using DHCP, uncomment the options for dynamic IP shown in the following figure, by editing the file */etc/network/interfaces*. In addition, you must comment the data for static IP (if they exist).



```
#dynamic ip address
#auto eth0
#iface eth0 inet dhcp
```

Figure 15. Dynamic IP

To set up the changes, save the changes in the file, exit and use the commands: **ifdown eth0** followed by **ifup eth0**.

2.6 TEST YOUR NETWORK

There are two options: (i) connect the virtual machine to a VPCS (this can be selected in the list of templates), or (ii) configure a simple network (recommended) as the next picture shows. A simple network will allow to check the connection easily. It should be possible to perform ***ping*** from PC-1 to PC-2 after these are configured.

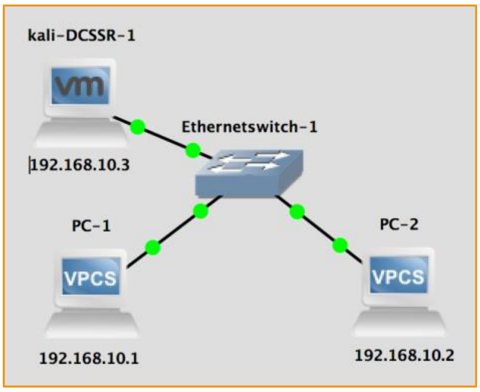
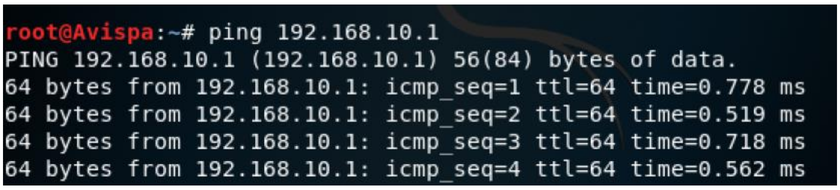


Figure 16. Simple network for testing



```
root@Avispa:~# ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=0.778 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=0.519 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=64 time=0.718 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=64 time=0.562 ms
```

Figure 17. Ping from Kali Linux VM

2.7 EXPORTING A GNS3 PROJECT

The following steps enable to export a GNS3 project while maintaing the configuration of the network elements.

The student must select: “File/Export portable project”, and then select the option for “include any base image”.

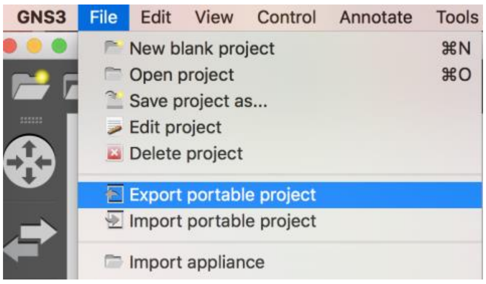


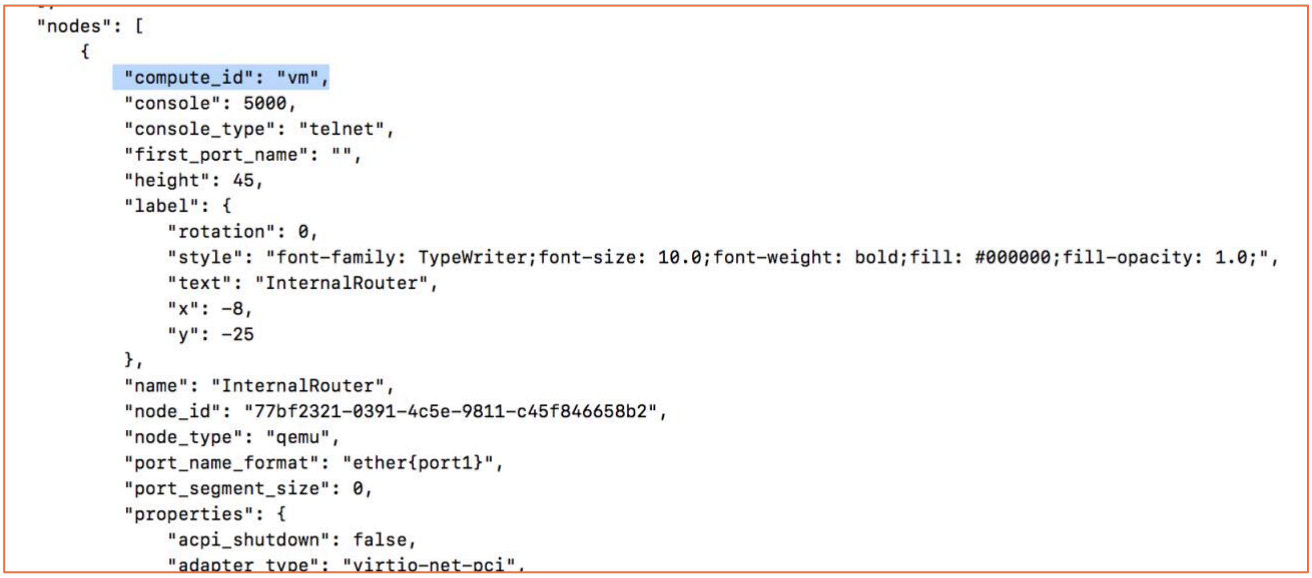
Figure 18. Export portable project

It is very important to check the new, exported project, in order to ensure that the exportation is correct.

2.8 DOWNLOADING GNS3 PROJECTS EXAMPLES FROM THE VIRTUAL CAMPUS

Some examples downloaded from the virtual campus may require some modifications in order to work. In particular, the files must be edited to change the local server with the server running in the GNS3 VM.

In order to change the server for any element in the project, the student must edit the file of the project and change the value of “compute_id” from “local” (local server) to “vm” (GNS3 VM).



```
"nodes": [
    {
        "compute_id": "vm",
        "console": 5000,
        "console_type": "telnet",
        "first_port_name": "",
        "height": 45,
        "label": {
            "rotation": 0,
            "style": "font-family: TypeWriter;font-size: 10.0;font-weight: bold;fill: #000000;fill-opacity: 1.0;",
            "text": "InternalRouter",
            "x": -8,
            "y": -25
        },
        "name": "InternalRouter",
        "node_id": "77bf2321-0391-4c5e-9811-c45f846658b2",
        "node_type": "qemu",
        "port_name_format": "ether{port1}",
        "port_segment_size": 0,
        "properties": {
            "acpi_shutdown": false,
            "adapter_type": "virtio-net-pci",
```

Figure 19. Change from local server to GNS3 VM server

2.9 FINAL REMARKS

After a change in the configuration of the virtual machine, it may be needed to restart the virtual machine to make the changes effective.

3 KALI TOOLS

This section shows examples of the use of some tools included in Kali linux.

3.1 INFORMATION GATHERING / NETWORK RECOGNAISSANCE

There is a list of features for information gathering in Kali Linux (Applications/Information gathering). The student can practise using any of these tools during the class. In this section, the use of some of these tools is described.

It must be noted that sometimes it is necessary to use a combination of these tools to get as much information as possible from the environment.

3.1.1 NMAP

Nmap is a powerful *command tool* for network reconnaissance (try ***namp -h*** to get a list of options to use *nmap*). Some options are listed in the following table but there are many more. The simplest way to use it is *nmap <ip>*, or *nmap <ip/mask>*.

Options	Description	Example
-T<*timing*>	Stands for timing (from 1 to 5). Default: -T3	`nmap -T4 192.10.1.251`
-A	Stands for "All": deep port scan, including OS identification, and attempts to find the applications listening on the ports, and the versions of those applications.	`nmap -T4 -A 192.10.1.251`
-v	Verbose (list more information). --v "very vervose"	`nmap -T4 -A -v 192.10.1.251`
-Pn	No ping.	`nmap -T4 -A -v -Pn 192.10.1.251`
-sC	Enable the most common scripts	`nmap -sC 192.10.1.251`
--script	Run a specific script scan	`(see example below)`
-sn	Ping scan. Disable port scan. Run a script scan without a port scan (only host discovery)	`nmap -V -sn 192.10.1.251`
-p<*port ranges*>	Only scan specified ports	`nmap -p22 192.10.1.251`

Zenmap is a GUI to use nmap. The application writes out the command line version of the command-line, and will help the student to learn the command-line flags used when making use of *nmap* in comman-line mode.

3.1.1.1 NMAP NETWORK SCRIPTING

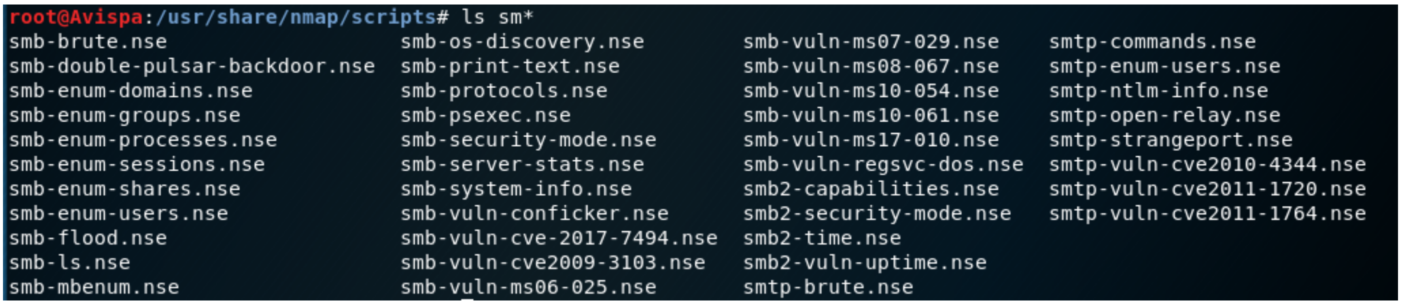
One interesting feature of *nmap* is that it is possible to create custom scripts (e.g. to check for new, recent vulnerabilities in the network). The student can find an exhaustive *script writing tutorial* and information about the *nmap scripting engine* (NSE) in the official web page of *nmap*: https://nmap.org/book/nse-tutorial.html, https://nmap.org/soc/Scripting.html. Some uses and examples are listed here: https://nmap.org/book/nse-usage.html. Note that the scripts are classified in different categories (e.g. "auth": bypass authentication credentials, "default": run when using the -sC or -A options).

Custom scripts need to be added to the NSE in order to work, usually in "/usr/share/nmap/scripts/". If the student wants to practice, in this website instructions can be found to download and use a custom script to identify if a server with *Server Message Block* (SMB) open is vulnerable to MS17-010 (e.g. used by WannaCry for propagation).

The student can have access to the ***package version*** of the script in this direction: https://svn.nmap.org/nmap/scripts/smb-vuln-ms17-010.nse. The command to use the script is as follows:

```
nmap -p445 --script smb-vuln-ms17-010 <IP_Network(target)>
```

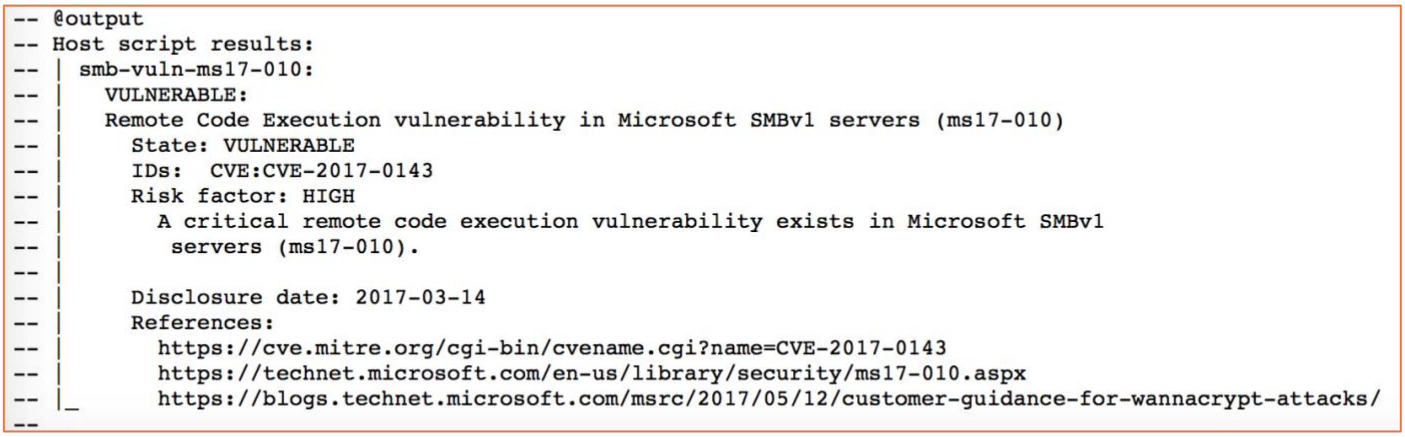
As the student can check, the script is currently available in the Kali Linux, because was included in the official list of NSE scripts.



```
root@Avispa:/usr/share/nmap/scripts# ls sm*
smb-brute.nse                  smb-os-discovery.nse          smb-vuln-ms07-029.nse      smtp-commands.nse
smb-double-pulsar-backdoor.nse smb-print-text.nse            smb-vuln-ms08-067.nse      smtp-enum-users.nse
smb-enum-domains.nse           smb-protocols.nse             smb-vuln-ms10-054.nse      smtp-ntlm-info.nse
smb-enum-groups.nse            smb-psexec.nse                smb-vuln-ms10-061.nse      smtp-open-relay.nse
smb-enum-processes.nse         smb-security-mode.nse         smb-vuln-ms17-010.nse      smtp-strangeport.nse
smb-enum-sessions.nse          smb-server-stats.nse          smb-vuln-regsvc-dos.nse    smtp-vuln-cve2010-4344.nse
smb-enum-shares.nse            smb-system-info.nse           smb2-capabilities.nse      smtp-vuln-cve2011-1720.nse
smb-enum-users.nse             smb-vuln-conficker.nse        smb2-security-mode.nse     smtp-vuln-cve2011-1764.nse
smb-flood.nse                  smb-vuln-cve-2017-7494.nse    smb2-time.nse
smb-ls.nse                     smb-vuln-cve2009-3103.nse     smb2-vuln-uptime.nse
smb-mbenum.nse                 smb-vuln-ms06-025.nse         smtp-brute.nse
```

Figure 20. List of NSE scripts that starring with "sm"

The output of the script if the machine is vulnerable should be similar to the following figure (***cat smb-vuln-ms17-010.nse***).

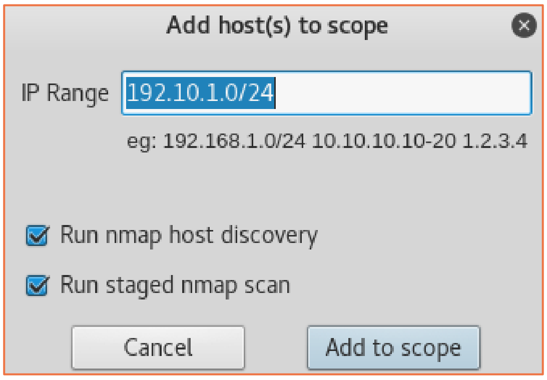


```
-- @output
-- Host script results:
-- | smb-vuln-ms17-010:
-- |   VULNERABLE:
-- |   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
-- |     State: VULNERABLE
-- |     IDs:  CVE:CVE-2017-0143
-- |     Risk factor: HIGH
-- |       A critical remote code execution vulnerability exists in Microsoft SMBv1
-- |        servers (ms17-010).
-- |
-- |     Disclosure date: 2017-03-14
-- |     References:
-- |       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
-- |       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
-- |_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
--
```

Figure 21. Host script results - Nmap *smb-vuln-ms17-010*

3.1.2 SPARTA

Sparta is a graphical tool for network scanning, enumeration and attack. This tool scans systems for open ports and services information. It also can detect existing vulnerabilities and provides access to tools for security testing. You can select *Sparta* using the menu *Applications/Information Gathering/Sparta* or using the terminal with the command ***sparta***. Then, click "Click here to add host(s) to scope" (left side of the GUI). Enter the IP or the range of IPs and click "Add to Scope".



Add host(s) to scope

IP Range 192.10.1.0/24

eg: 192.168.1.0/24 10.10.10.10-20 1.2.3.4

☑ Run nmap host discovery

☑ Run staged nmap scan

Figure 22.Add host(s) to scope in Sparta

For example, given the network shown in Figure 23, if the student uses Sparta in order to scan the network 192.10.1.0/24, then the output will show information about the hosts in the network.

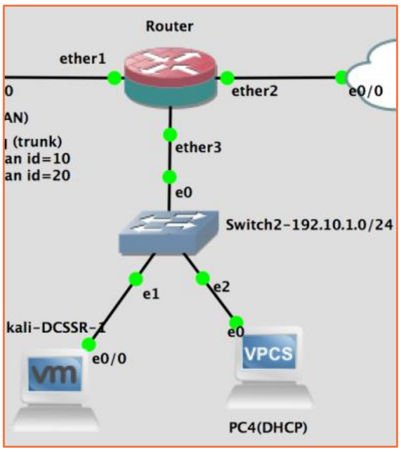
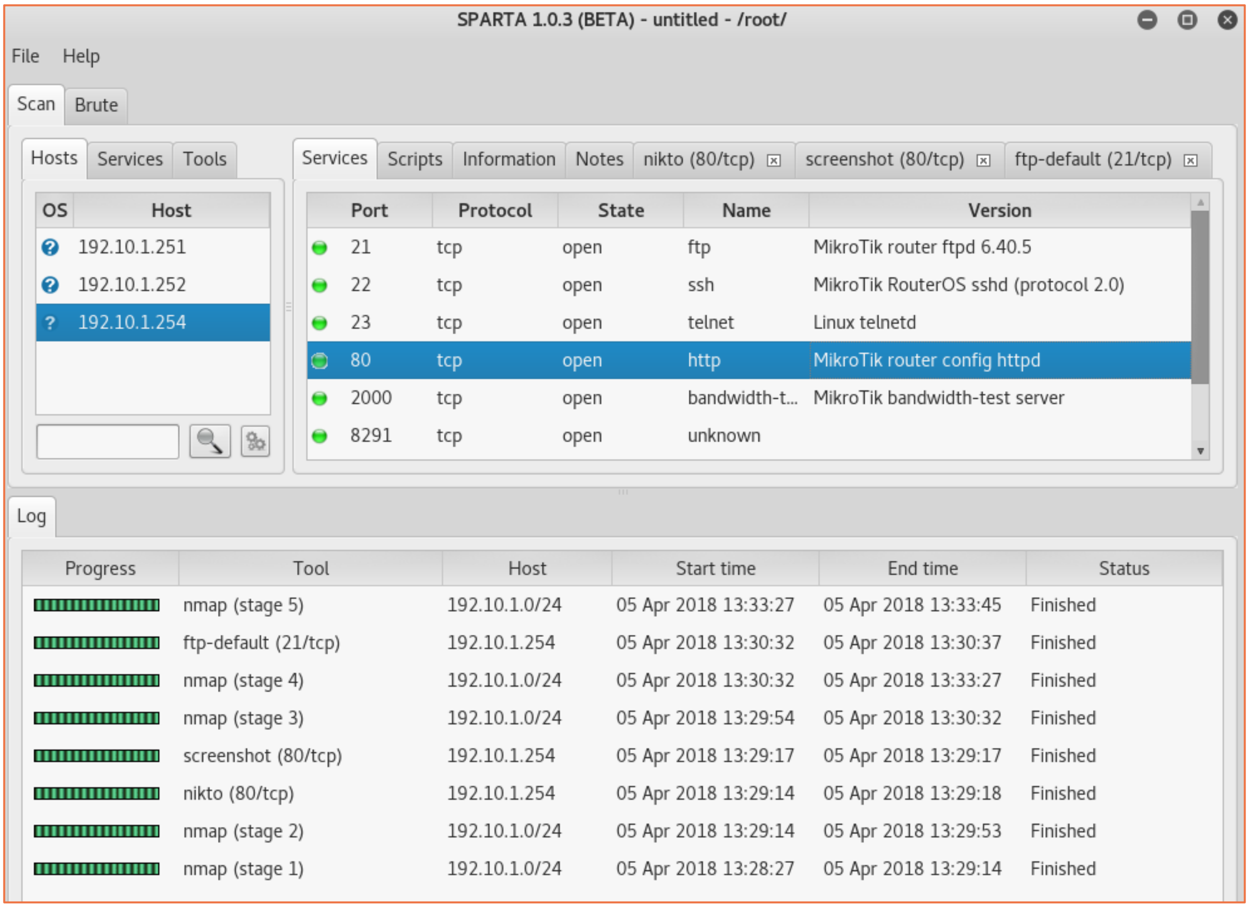


Figure 23. Subnet for testing with Sparta



OS	Host
?	192.10.1.251
?	192.10.1.252
?	192.10.1.254

	Port	Protocol	State	Name	Version
●	21	tcp	open	ftp	MikroTik router ftpd 6.40.5
●	22	tcp	open	ssh	MikroTik RouterOS sshd (protocol 2.0)
●	23	tcp	open	telnet	Linux telnetd
●	80	tcp	open	http	MikroTik router config httpd
●	2000	tcp	open	bandwidth-t...	MikroTik bandwidth-test server
●	8291	tcp	open	unknown	

Progress	Tool	Host	Start time	End time	Status
	nmap (stage 5)	192.10.1.0/24	05 Apr 2018 13:33:27	05 Apr 2018 13:33:45	Finished
	ftp-default (21/tcp)	192.10.1.254	05 Apr 2018 13:30:32	05 Apr 2018 13:30:37	Finished
	nmap (stage 4)	192.10.1.0/24	05 Apr 2018 13:30:32	05 Apr 2018 13:33:27	Finished
	nmap (stage 3)	192.10.1.0/24	05 Apr 2018 13:29:54	05 Apr 2018 13:30:32	Finished
	screenshot (80/tcp)	192.10.1.254	05 Apr 2018 13:29:17	05 Apr 2018 13:29:17	Finished
	nikto (80/tcp)	192.10.1.254	05 Apr 2018 13:29:14	05 Apr 2018 13:29:18	Finished
	nmap (stage 2)	192.10.1.0/24	05 Apr 2018 13:29:14	05 Apr 2018 13:29:53	Finished
	nmap (stage 1)	192.10.1.0/24	05 Apr 2018 13:28:27	05 Apr 2018 13:29:14	Finished

Figure 24. Output of Sparta for 192.10.1.0/24

Note that you can find information about the router Mikrotik. Try to open the page to configure the router.

Finally, note that Sparta is using *nmap* to perform the tests, and also *nikto*. The second one is a web server scanner which performs comprehensive tests against web servers for items. Nikto is not designed as a stealthy tool. It will test a web server in the quickest time possible, and is obvious in log files or to an IPS/IDS.

3.1.3 ETHERAPE (NOT IN KALI, BUT IN YOUR KALI)

This application has been installed in kali linux in order to help to the network reconnaissance. The application shows the traffic between the nodes in the network by using a graphical interface, as next figure shows.

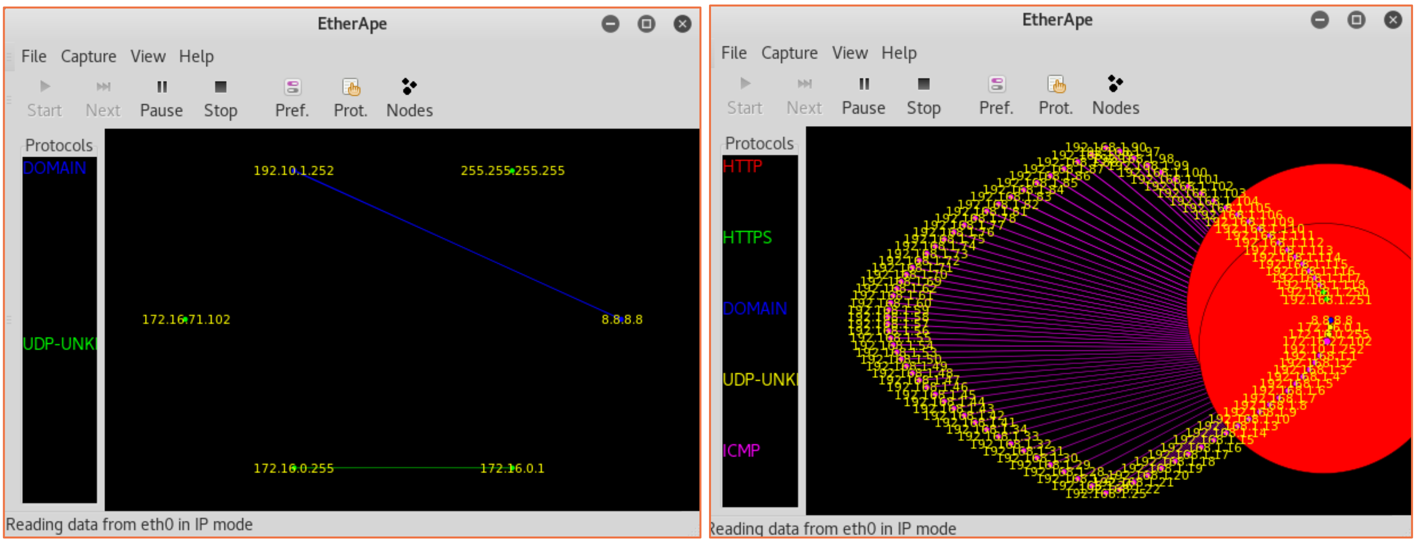


Figure 25. EtherApe outputs

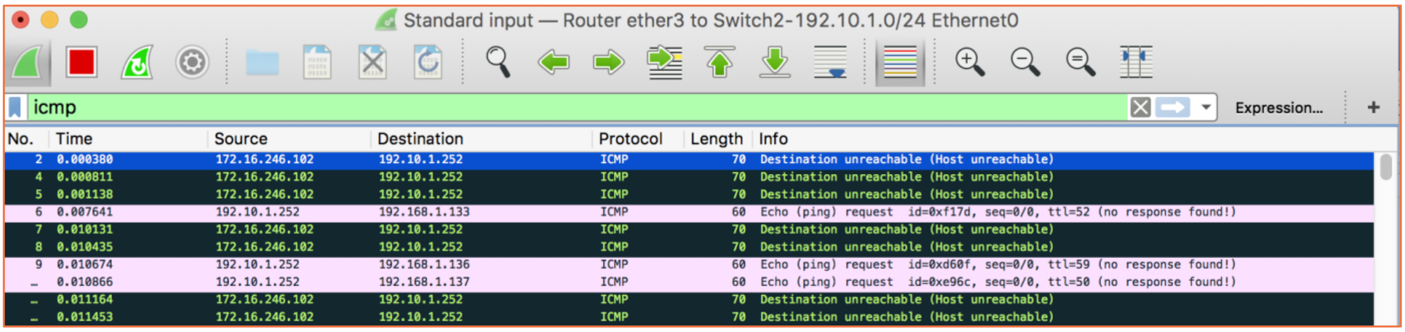
The student can open one of the sniffers before executing etherape and check the connections while the application is working. When the traffic increases, the lines between the hosts are wider.

3.2 NETWORK SNIFFERS

There is a list of applications for network sniffing in *Applications/Sniffing & Spoofing*. The student can practise using any of these tools during the class. In this section, the use of some of these tools is described.

3.2.1 WIRESHARK

Wireshark is "the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions." (*Wireshark official web site*).

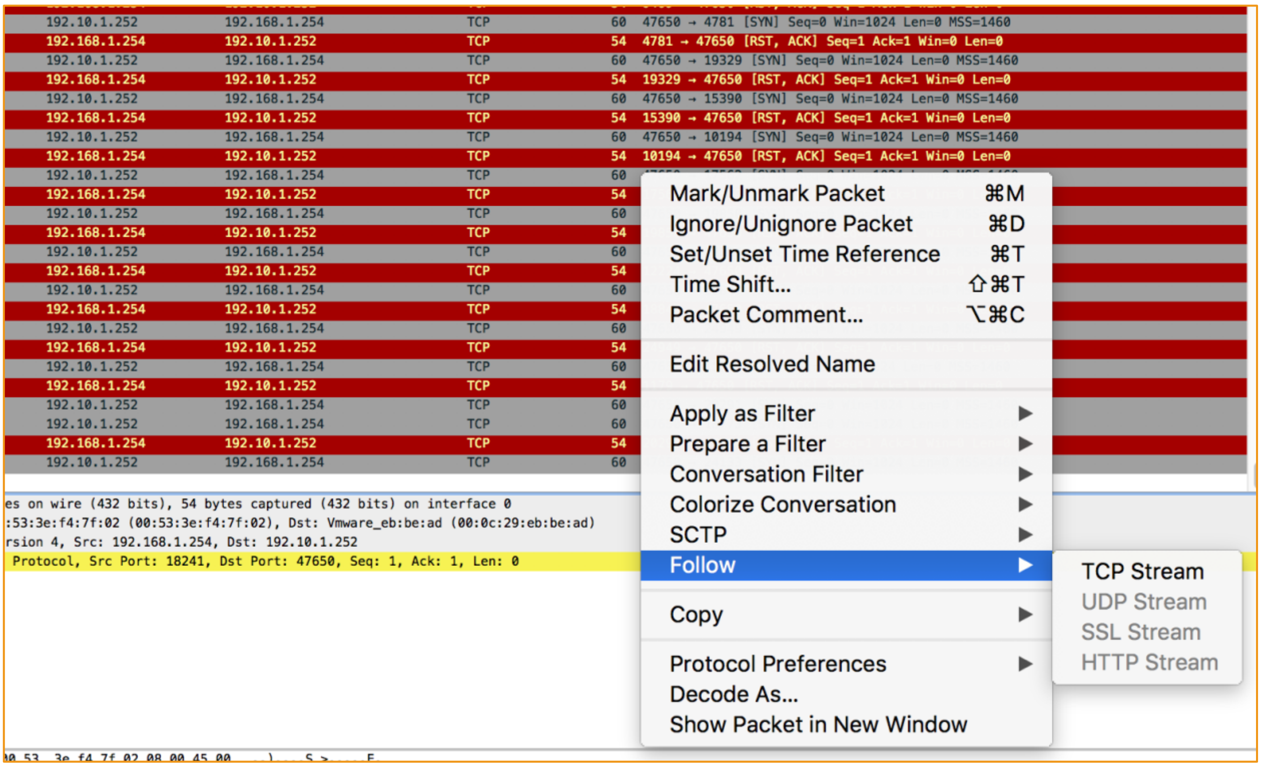

Standard input — Router ether3 to Switch2-192.10.1.0/24 Ethernet0
icmp
Expression...
+

```
No.  Time      Source          Destination     Protocol  Length  Info
  2  0.000380  172.16.246.102  192.10.1.252    ICMP          70  Destination unreachable (Host unreachable)
  4  0.000811  172.16.246.102  192.10.1.252    ICMP          70  Destination unreachable (Host unreachable)
  5  0.001138  172.16.246.102  192.10.1.252    ICMP          70  Destination unreachable (Host unreachable)
  6  0.007641  192.10.1.252    192.168.1.133   ICMP          60  Echo (ping) request  id=0xf17d, seq=0/0, ttl=52 (no response found!)
  7  0.010131  172.16.246.102  192.10.1.252    ICMP          70  Destination unreachable (Host unreachable)
  8  0.010435  172.16.246.102  192.10.1.252    ICMP          70  Destination unreachable (Host unreachable)
  9  0.010674  192.10.1.252    192.168.1.136   ICMP          60  Echo (ping) request  id=0xd60f, seq=0/0, ttl=59 (no response found!)
  …  0.010866  192.10.1.252    192.168.1.137   ICMP          60  Echo (ping) request  id=0xe96c, seq=0/0, ttl=50 (no response found!)
  …  0.011164  172.16.246.102  192.10.1.252    ICMP          70  Destination unreachable (Host unreachable)
  …  0.011453  172.16.246.102  192.10.1.252    ICMP          70  Destination unreachable (Host unreachable)
```

Figure 26. Output of *Wireshark* after enabling the filter for ICMP.

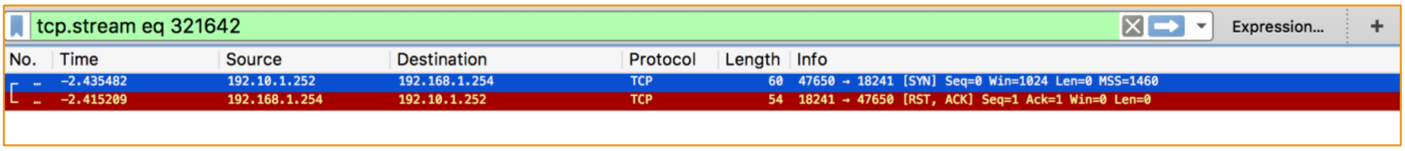
This tool allows network capture, filtering (https://wiki.wireshark.org/DisplayFilters), show the communication between the network elements in a graphical way, and many other features listed in the official web site: https://www.wireshark.org/about.html.

Between the wireshark features, it is possible to "follow a TCP stream" as the following figures show. This is useful to see all the packets in the same stream.



```
192.10.1.252     192.168.1.254    TCP   60  47650 → 4781 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.1.254    192.10.1.252     TCP   54  4781 → 47650 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.10.1.252     192.168.1.254    TCP   60  47650 → 19329 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.1.254    192.10.1.252     TCP   54  19329 → 47650 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.10.1.252     192.168.1.254    TCP   60  47650 → 15390 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.1.254    192.10.1.252     TCP   54  15390 → 47650 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.10.1.252     192.168.1.254    TCP   60  47650 → 10194 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.1.254    192.10.1.252     TCP   54  10194 → 47650 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.10.1.252     192.168.1.254    TCP   60
192.168.1.254    192.10.1.252     TCP   54
192.10.1.252     192.168.1.254    TCP   60
192.168.1.254    192.10.1.252     TCP   54
192.10.1.252     192.168.1.254    TCP   60
192.168.1.254    192.10.1.252     TCP   54
192.10.1.252     192.168.1.254    TCP   60
192.168.1.254    192.10.1.252     TCP   54
192.10.1.252     192.168.1.254    TCP   60
192.168.1.254    192.10.1.252     TCP   54
192.10.1.252     192.168.1.254    TCP   60
192.168.1.254    192.10.1.252     TCP   54
192.10.1.252     192.168.1.254    TCP   60
192.10.1.252     192.168.1.254    TCP   60
192.168.1.254    192.10.1.252     TCP   54
192.10.1.252     192.168.1.254    TCP   60

es on wire (432 bits), 54 bytes captured (432 bits) on interface 0
:53:3e:f4:7f:02 (00:53:3e:f4:7f:02), Dst: Vmware_eb:be:ad (00:0c:29:eb:be:ad)
rsion 4, Src: 192.168.1.254, Dst: 192.10.1.252
 Protocol, Src Port: 18241, Dst Port: 47650, Seq: 1, Ack: 1, Len: 0
```

Figure 27. Follow TCP stream option



```
tcp.stream eq 321642

No.  Time        Source          Destination     Protocol  Length  Info
     -2.435482   192.10.1.252    192.168.1.254   TCP       60      47650 → 18241 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
     -2.415209   192.168.1.254   192.10.1.252    TCP       54      18241 → 47650 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

Figure 28. Follow TCP stream results

3.2.2 ETTERCAP (ALSO A SPOOFING NETWORK TRAFFIC TOOL)

Ettercap is an application that allows to **capture network traffic** (sniffer) but also is a very good tool to perform ***spoofing***. This tool is listed in this section and not in the following section because of the specific location in Kali linux. Using this application is possible to capture, modify and inject network traffic. Ettercap enables the capture of network traffic in switched networks. This means that even if there is a bridge it could capture traffic (subject to the type of network and additional security configuration). It is possible to run this application in graphical mode with the option "-G".

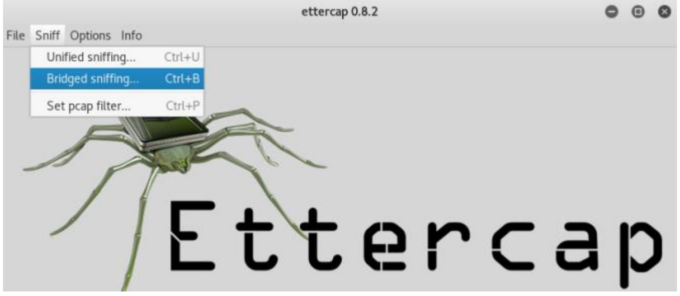


Figure 29. Sniffing options in *Ettercap*

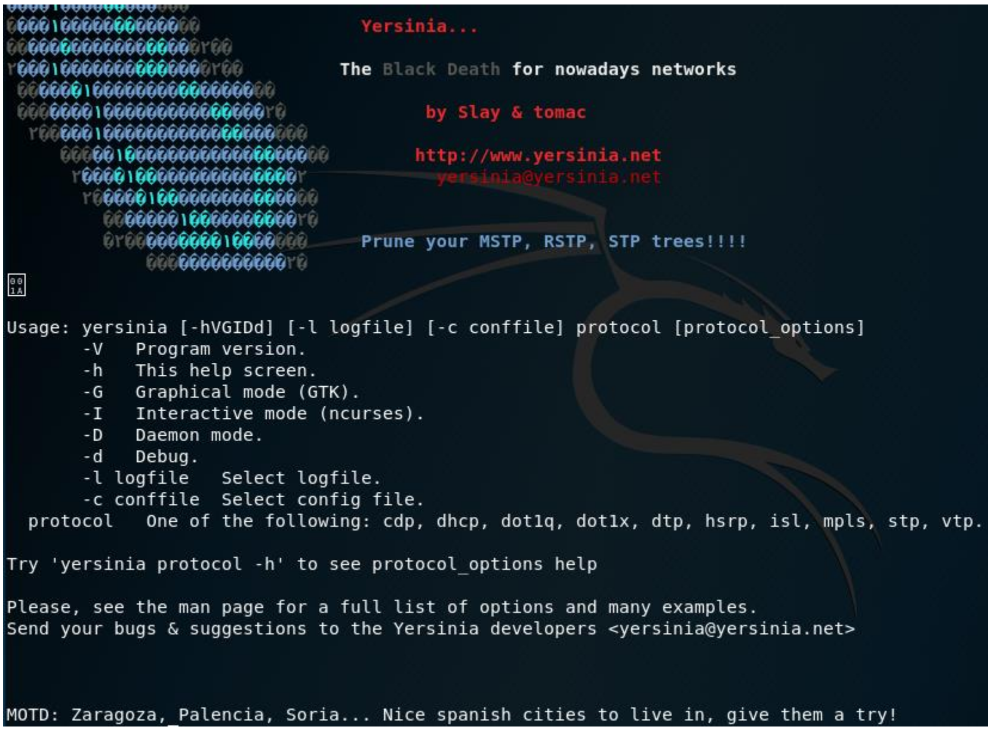
Some MITM attacks that can be performed are: ARP poisoning, ICMP redirection, Port stealing, DHCP spoofing.

3.3 SPOOFING & MITM

Specific tools for *spoofing & MITM* can be found in "*Applications/Sniffing & Spoofing/Spoofing & MITM*". In the following, Yersinia is presented as one of these tools. The student can practise using any of these tools during the class.

3.3.1 YERSINIA

Yersinia is a network tool designed to take advantage of some weaknesses in different network protocols (official web site: http://www.yersinia.net).



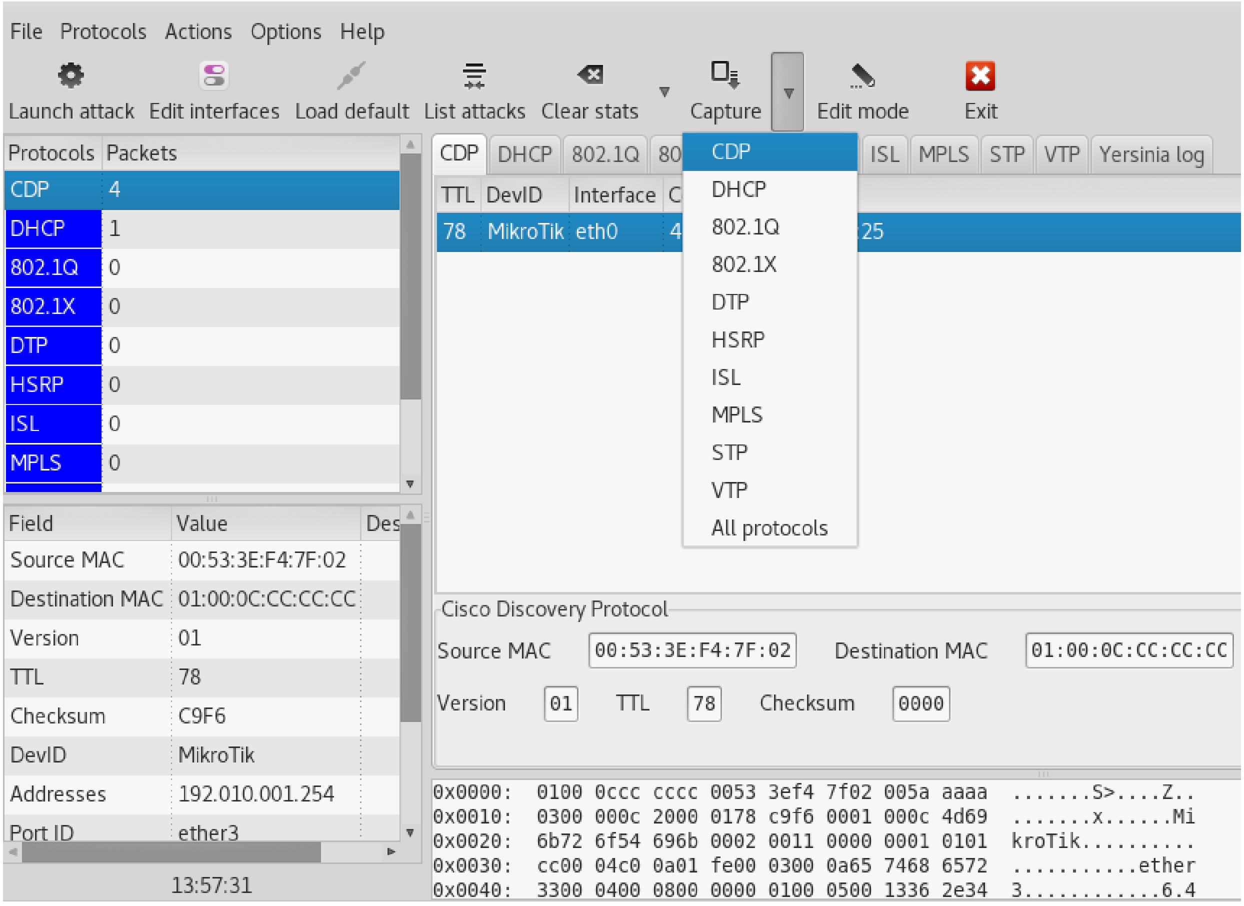
```
                         Yersinia...

                      The Black Death for nowadays networks

                              by Slay & tomac

                            http://www.yersinia.net
                              yersinia@yersinia.net


                         Prune your MSTP, RSTP, STP trees!!!!


Usage: yersinia [-hVGIDd] [-l logfile] [-c conffile] protocol [protocol_options]
       -V   Program version.
       -h   This help screen.
       -G   Graphical mode (GTK).
       -I   Interactive mode (ncurses).
       -D   Daemon mode.
       -d   Debug.
       -l logfile   Select logfile.
       -c conffile  Select config file.
  protocol   One of the following: cdp, dhcp, dot1q, dot1x, dtp, hsrp, isl, mpls, stp, vtp.

Try 'yersinia protocol -h' to see protocol_options help

Please, see the man page for a full list of options and many examples.
Send your bugs & suggestions to the Yersinia developers <yersinia@yersinia.net>


MOTD: Zaragoza, Palencia, Soria... Nice spanish cities to live in, give them a try!
```

Figure 30. *Yersinia* options

Yersinia is also a solid framework for analysing and testing the deployed networks and systems. The student can run this application in graphical mode (-G). This tool implements attacks for the following network protocols:

- Scanning Tree Protocol (STP)
- Cisco Discovery Protocol (CDP)
- Dynamic Trunking Protocol (DTP)
- Dynamic Host Configuration Protocol (DHCP)
- Host Standby Router Protocol (HSRP)
- IEEE 802.1Q
- IEEE 802.1X
- Inter-Switch Link Protocol (ISL)
- VLAN Trunking Protocol (VTP)

For example, the following figure shows the results after selecting the option of "capturing CDP".



Protocols	Packets
CDP	4
DHCP	1
802.1Q	0
802.1X	0
DTP	0
HSRP	0
ISL	0
MPLS	0

TTL	DevID	Interface	C	
78	MikroTik	eth0	4	25

Field	Value	Des
Source MAC	00:53:3E:F4:7F:02	
Destination MAC	01:00:0C:CC:CC:CC	
Version	01	
TTL	78	
Checksum	C9F6	
DevID	MikroTik	
Addresses	192.010.001.254	
Port ID	ether3	

13:57:31

Cisco Discovery Protocol

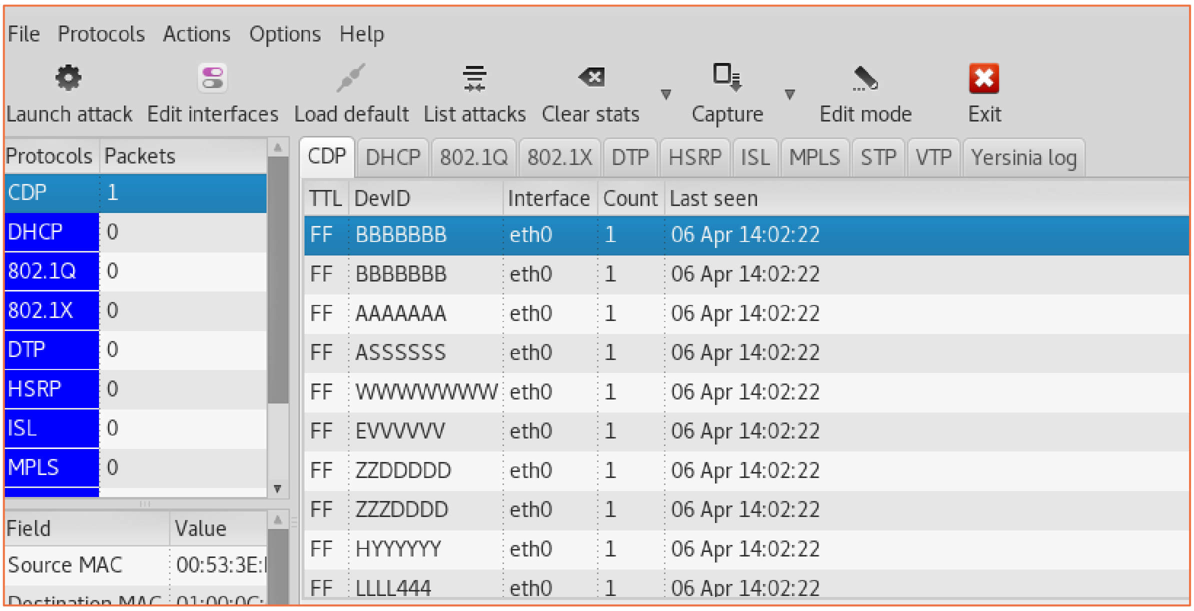
Source MAC 00:53:3E:F4:7F:02 Destination MAC 01:00:0C:CC:CC:CC

Version 01 TTL 78 Checksum 0000

```
0x0000:  0100 0ccc cccc 0053 3ef4 7f02 005a aaaa  .......S>....Z..
0x0010:  0300 000c 2000 0178 c9f6 0001 000c 4d69  .......x......Mi
0x0020:  6b72 6f54 696b 0002 0011 0000 0001 0101  kroTik..........
0x0030:  cc00 04c0 0a01 fe00 0300 0a65 7468 6572  ...........ether
0x0040:  3300 0400 0800 0000 0100 0500 1336 2e34  3...........6.4
```

Figure 31. *Yersinia*: capturing CDP packets

It is also possible to launch attacks. For example, you can try to perform DoS attacks against the Mikrotik router, knowing that it uses CDP. Choose "Launch Attack/CDP" and "flooding CDP table" gives the following results. The student can check if the router is operative after the attack. Likely, this attack will affect to other elements in the network using this protocol (Cisco protocol). This means that this attack will affect to a large number of devices if appropriate countermeasures are not taken.



Protocols	Packets
CDP	1
DHCP	0
802.1Q	0
802.1X	0
DTP	0
HSRP	0
ISL	0
MPLS	0

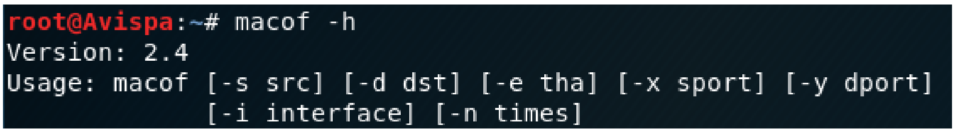
TTL	DevID	Interface	Count	Last seen
FF	BBBBBBB	eth0	1	06 Apr 14:02:22
FF	BBBBBBB	eth0	1	06 Apr 14:02:22
FF	AAAAAAA	eth0	1	06 Apr 14:02:22
FF	ASSSSSS	eth0	1	06 Apr 14:02:22
FF	WWWWWWW	eth0	1	06 Apr 14:02:22
FF	EVVVVVV	eth0	1	06 Apr 14:02:22
FF	ZZDDDDD	eth0	1	06 Apr 14:02:22
FF	ZZZDDDD	eth0	1	06 Apr 14:02:22
FF	HYYYYYY	eth0	1	06 Apr 14:02:22
FF	LLLL444	eth0	1	06 Apr 14:02:22

Field	Value
Source MAC	00:53:3E:
Destination MAC	01:00:0C:

Figure 32. *Yersinia:* Performing a *flooding CDP table* attack

3.3.2 MACOF

This tool is not listed as favourite in Kali linux, but is very interesting (and easy to use) in order to launch ***MAC address flooding*** attacks against switches. The tool floods switches with invalid source MAC addresses. Figure 33 shows the options to use macof.



```
root@Avispa:~# macof -h
Version: 2.4
Usage: macof [-s src] [-d dst] [-e tha] [-x sport] [-y dport]
             [-i interface] [-n times]
```

Figure 33. *macof* options

Options	Description
-s	Source IP address
-d	Destination IP address
-e	Target hardware address (tha)
-x	TCP source port
-y	TCP destination port
-i	Interface to send on
-n	Number of packets to send (**infinite by default)**

Some switches recover their initial state after some time interval. This can be bypassed by configuring macof in burst mode:

```
while [ 1 ] ; do macof -d 192.10.1.1 -n 100000 ; sleep 50 ; done
```

This tool is part of the packet *dsniff*, which contains tools for *network sniffing*, some of which are listed in the following table. The student can use the command line to get more information about these tools (-h option).

Tool	Description
macof	Causes LAN switch to fail-open (i.e. Act as a hub and broadcast traffic to all hosts)
arpspoof	Redirect packets on a LAN to defeat the host-isolating behaviour of the switch
dnsspoof	Forges replies to DNS queries
tcpkill	Kills specified in-progress TCP connections
tcpnice	Slows down specified TCP connections

3.3.2.1 Practical example: MAC address flooding attack

The following example shows the output for a MAC address flooding attack using *macof*. **Objective: it must be demonstrated that the attacker can force the switch to act as a hub, in order to receive all the packets from other members in the network.**

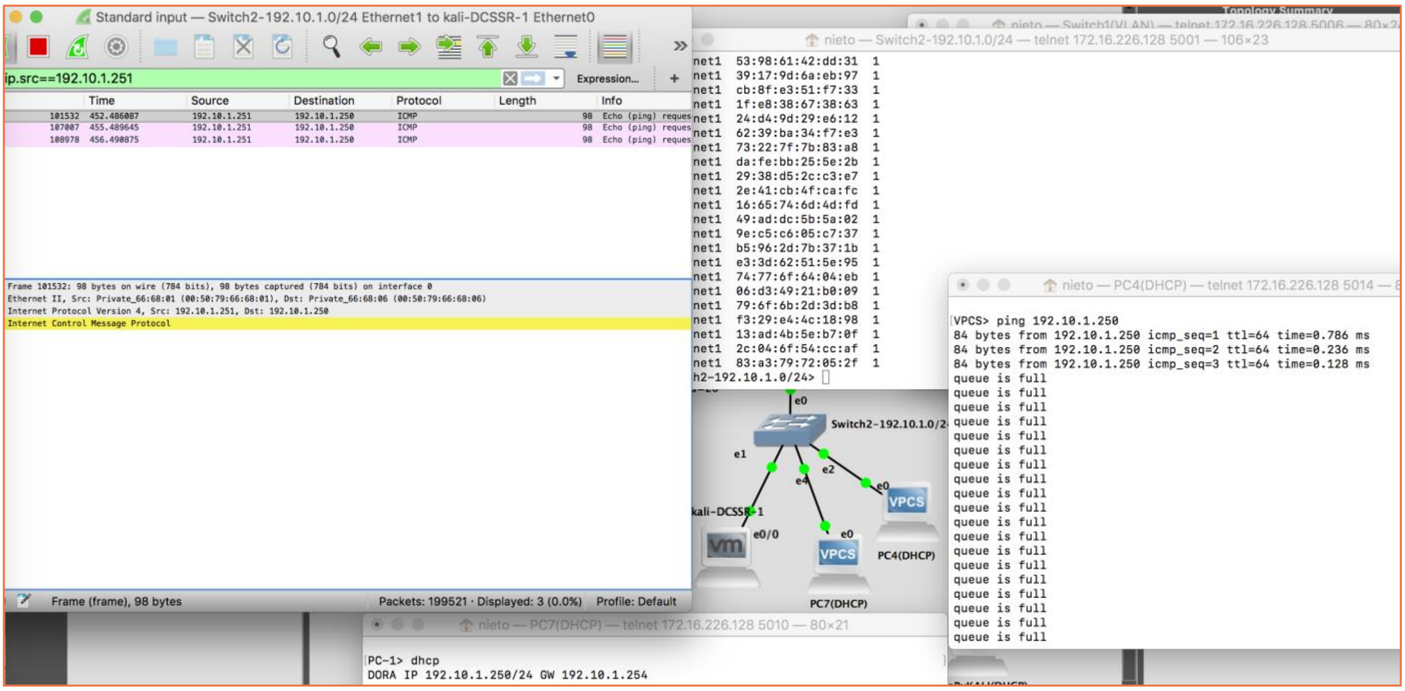
Steps:

1.- Kali-DSSR-1 (the attacker), PC4 and PC7 are connected to the same switch. **Note: The student must be prepared and annotate the IP of PC4 and PC7 before starting**. In our test, PC4 IP = 192.10.1.251 and PC7 IP = 192.10.1.250.

2.- Prepare the *network sniffer* (e.g. wireshark in this case). The student has two options: 1) open wireshark in the attacker's virtual machine or 2) open wireshark using GNS3, in the link between the Kali Linux and the switch. The effect is the same, but the second option is more "comfortable". Use the filter in order to obtain the desired packets to demonstrate that the attack is working. In this case, **ip.src=192.10.1.251** (IP of PC4).

3.- The attacker executes the command **"macof -d 10.10.1.253"**. The IP is irrelevant; it is only an excuse to send a lot of traffic out of the network.

4.- Then, if a **ping** is executed from PC4 to PC7. Note that the attacker is able to receive this information that is not directed to his computer (destination address is 192.10.1.250, which is the IP of PC7 in this test). **This is possible because the switch is acting as a hub.**



Standard input — Switch2-192.10.1.0/24 Ethernet1 to kali-DCSSR-1 Ethernet0

ip.src==192.10.1.251

```
         Time         Source         Destination    Protocol   Length  Info
101532   452.486087   192.10.1.251   192.10.1.250   ICMP           98  Echo (ping) reques
107007   455.489645   192.10.1.251   192.10.1.250   ICMP           98  Echo (ping) reques
108978   456.490875   192.10.1.251   192.10.1.250   ICMP           98  Echo (ping) reques
```

```
Frame 101532: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Private_66:68:06 (00:50:79:66:68:06)
Internet Protocol Version 4, Src: 192.10.1.251, Dst: 192.10.1.250
Internet Control Message Protocol
```

Frame (frame), 98 bytes   Packets: 199521 · Displayed: 3 (0.0%)   Profile: Default

nieto — Switch2-192.10.1.0/24 — telnet 172.16.226.128 5001 — 106×23

```
net1  53:98:61:42:dd:31  1
net1  39:17:9d:6a:eb:97  1
net1  cb:8f:e3:51:f7:33  1
net1  1f:e8:38:67:38:63  1
net1  24:d4:9d:29:e6:12  1
net1  62:39:ba:34:f7:e3  1
net1  73:22:7f:7b:83:a8  1
net1  da:fe:bb:25:5e:2b  1
net1  29:38:d5:2c:c3:e7  1
net1  2e:41:cb:4f:ca:fc  1
net1  16:65:74:6d:4d:fd  1
net1  49:ad:dc:5b:5a:02  1
net1  9e:c5:c6:05:c7:37  1
net1  b5:96:2d:7b:37:1b  1
net1  e3:3d:62:51:5e:95  1
net1  74:77:6f:64:04:eb  1
net1  06:d3:49:21:b0:09  1
net1  79:6f:6b:2d:3d:b8  1
net1  f3:29:e4:4c:18:98  1
net1  13:ad:4b:5e:b7:0f  1
net1  2c:04:6f:54:cc:af  1
net1  83:a3:79:72:05:2f  1
h2-192.10.1.0/24>
```

nieto — PC4(DHCP) — telnet 172.16.226.128 5014

```
VPCS> ping 192.10.1.250
84 bytes from 192.10.1.250 icmp_seq=1 ttl=64 time=0.786 ms
84 bytes from 192.10.1.250 icmp_seq=2 ttl=64 time=0.236 ms
84 bytes from 192.10.1.250 icmp_seq=3 ttl=64 time=0.128 ms
queue is full
queue is full
queue is full
queue is full
queue is full
queue is full
queue is full
queue is full
queue is full
queue is full
queue is full
queue is full
queue is full
queue is full
queue is full
queue is full
queue is full
queue is full
queue is full
```

nieto — PC7(DHCP) — telnet 172.16.226.128 5010 — 80×21

```
PC-1> dhcp
DORA IP 192.10.1.250/24 GW 192.10.1.254
```

Figure 34. Results of the *MAC address flooding* attack

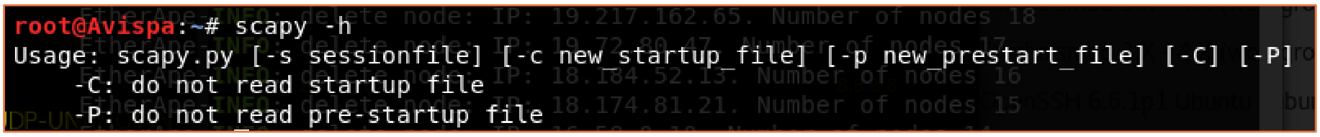
3.4 PACKET MANIPULATION

There are multiple tools that can be used for *packet manipulation*. Even some network sniffers enable this functionality (e.g. ettercape). In this section, some specific tools for packet manipulation are detailed. Note that, unlike the previous sections, this section has not a direct correspondence with the classification of applications in Kali Linux.

3.4.1 SCAPY

This tool is not listed as favourite in Kali linux, but is extremely interesting. *Scapy* is a ***packet manipulation*** tool written in Python (official website: http://www.secdev.org/projects/scapy/, online documentation: http://scapy.readthedocs.io/en/latest/). This tool is used for multiple purposes (e.g. build packets with a specific format to check IDS/IPSs). The student can find a summary with the main functionalities of scapy in the *scapy cheat sheet* developed by SANS (https://blogs.sans.org/pen-testing/files/2016/04/ScapyCheatSheet_v0.2.pdf).

Scapy provides an interactive shell in order to execute a rich set of functions. In order to use the interactive terminal only, call "scapy" in the command line. If the student wishes to use a specific file to be interpreted by *scapy*, then the following options may be useful.



```
root@Avispa:~# scapy -h
Usage: scapy.py [-s sessionfile] [-c new_startup_file] [-p new_prestart_file] [-C] [-P]
    -C: do not read startup file
    -P: do not read pre-startup file
```

Figure 35. *scapy.py* options

The following table describes some of the functions that will be used in some examples.

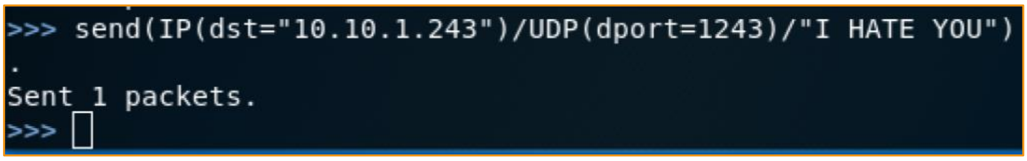
Function	Description	Example
IP	IP packet	`a=IP(dst="4.5.6.7",src="1.2.3.4", ttl=10)`
diplay	Show information about the object	`a.display()`
TCP	TCP packet	`a=TCP(dport=80, flags=CS")`
/	Composition operator between two layers	`IP()/TCP()`
send	Send a packet or list of packets	`send(IP())`
sr	Sends and receives without a custom ether() layer	`b=sr(a,retry=5,timeout=1.5, iface="eth0", filter="host 1.2.3.4 and port 80")`
sniff	Sniff using Berkley packet filters	`b=sniff(filter="host 1.1.1.1")`
rdpcap	Reading packets from a pcap	`rdpcap("filename.pcap")`
wrpcap	Writing packets to a pcap	`wrpcap("filename.pcap", packets)`
exit	Exit from scapy	`exit()`
ICMP	ICMP packet	`ICMP()`

For example, the following code builds an IP packet using *scapy*.

```
>>> a=IP(ttl=10)
>>> a
< IP ttl=10 |>
>>> a.src
’127.0.0.1’
>>> a.dst="192.168.1.1"
>>> a
< IP ttl=10 dst=192.168.1.1 |>
>>> a.src
’192.168.8.14’
>>> del(a.ttl)
>>> a
< IP dst=192.168.1.1 |>
>>> a.ttl
64
```

Note that the parameter “a” is used to create the IP packet and is modified to complete the information of the packet. This example can be found in: http://scapy.readthedocs.io/en/latest/usage.html#generating-sets-of-packets.

This tutorial shows how to send content in a IP packet using Scapy:
https://searchsecurity.techtarget.com/tip/Scapy-tutorial-How-to-use-Scapy-to-test-Snort-rules



```
>>> send(IP(dst="10.10.1.243")/UDP(dport=1243)/"I HATE YOU")
.
Sent 1 packets.
>>> 
```

Figure 36. Scapy - Sending content in the payload of a IP packet

3.4.1.1 Practical Example: IP Spoofing attack using Scapy

The goal is to trick a node in the network (A) into sending a legitimate packet to another node (B). To do that, the attacker (M), will impersonate A.

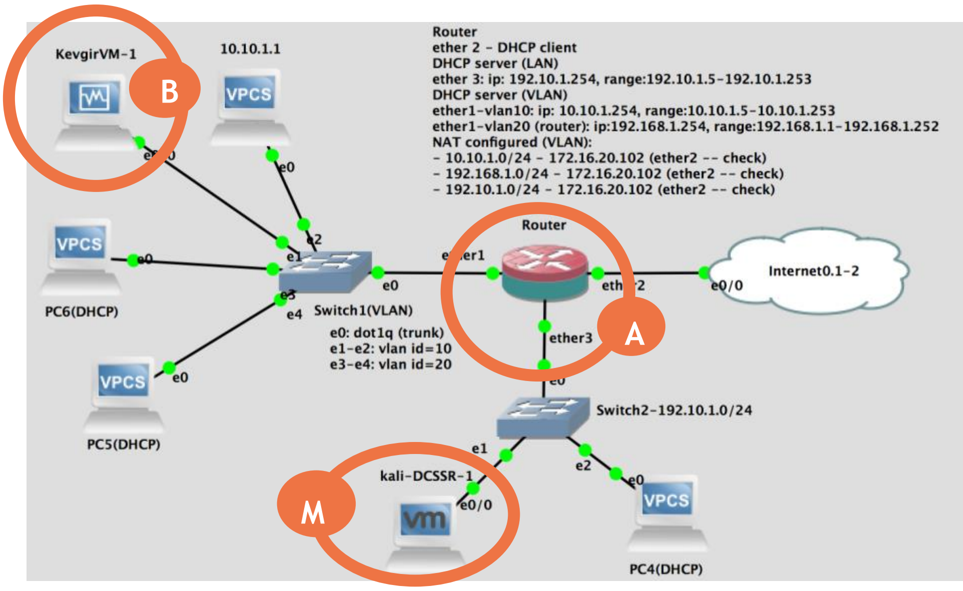

KevgirVM-1
B
10.10.1.1
VPCS
e0
e0
Router
ether 2 - DHCP client
DHCP server (LAN)
ether 3: ip: 192.10.1.254, range:192.10.1.5-192.10.1.253
DHCP server (VLAN)
ether1-vlan10: ip: 10.10.1.254, range:10.10.1.5-10.10.1.253
ether1-vlan20 (router): ip:192.168.1.254, range:192.168.1.1-192.168.1.252
NAT configured (VLAN):
- 10.10.1.0/24 - 172.16.20.102 (ether2 -- check)
- 192.168.1.0/24 - 172.16.20.102 (ether2 -- check)
- 192.10.1.0/24 - 172.16.20.102 (ether2 -- check)
VPCS
e0
PC6(DHCP)
e1
e2
e3
e4
e0
Switch1(VLAN)
e0: dot1q (trunk)
e1-e2: vlan id=10
e3-e4: vlan id=20
Router
ether1
ether2
ether3
A
e0/0
Internet0.1-2
VPCS
e0
PC5(DHCP)
e0
Switch2-192.10.1.0/24
e1
e2
kali-DCSSR-1
e0/0
M
vm
e0
VPCS
PC4(DHCP)

Figure 37. Practical example using *Scapy*: IP spoofing attack - Kali (M), Router (A), Kevgir (B)

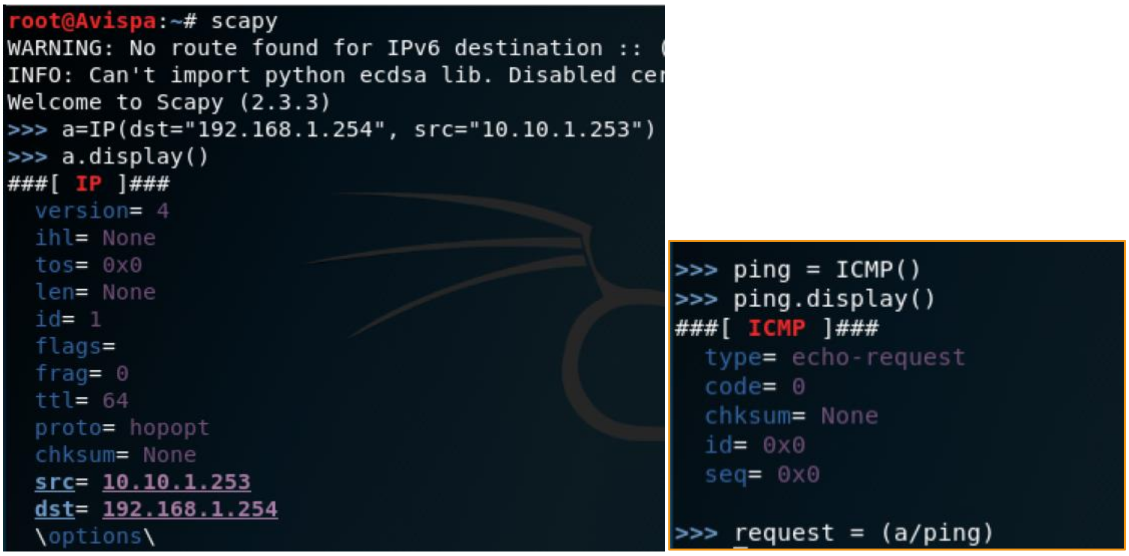
Steps:

1.- Prepare the sniffer (wireshark) between the final victim **B** that will receive the packet from **A**. A will be the router, with IP 192.168.1.254, and B will be the Kevgir VM, with IP 10.10.1.253.

2.- In Kali-DCSSR (the attacker, M):

2.1.- Construct the IP packet, with destination address (dst) the IP of the node that will be tricked. In this case, the tricked node will be the router, with IP 192.168.1.254. The source address (src) will be the second victim, who will receive an unsolicited response. In this case, the second victim is the Kevgir VM, with IP 10.10.1.253.

2.2.- Construct the ICMP packet and add it to the IP packet using the operator "/". The result of this operation is the request to be sent.

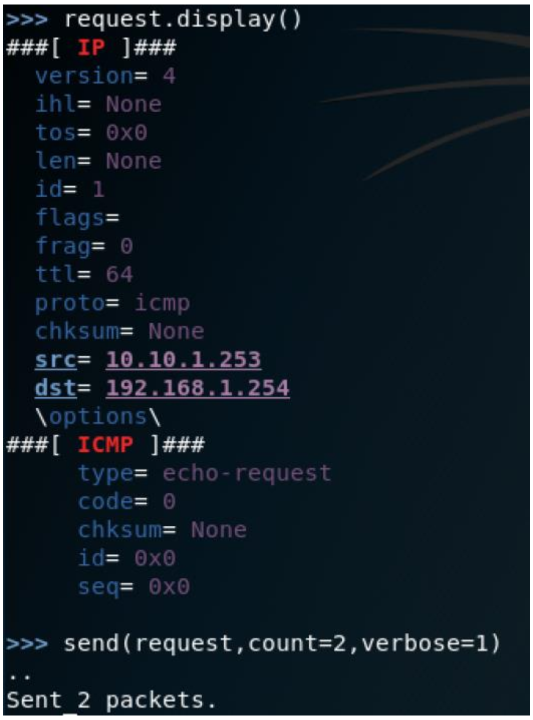


```
root@Avispa:~# scapy
WARNING: No route found for IPv6 destination :: (
INFO: Can't import python ecdsa lib. Disabled cer
Welcome to Scapy (2.3.3)
>>> a=IP(dst="192.168.1.254", src="10.10.1.253")
>>> a.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  chksum= None
  src= 10.10.1.253
  dst= 192.168.1.254
  \options\
```

```
>>> ping = ICMP()
>>> ping.display()
###[ ICMP ]###
  type= echo-request
  code= 0
  chksum= None
  id= 0x0
  seq= 0x0

>>> request = (a/ping)
```

Figure 38. Construct the IP packet with Scapy

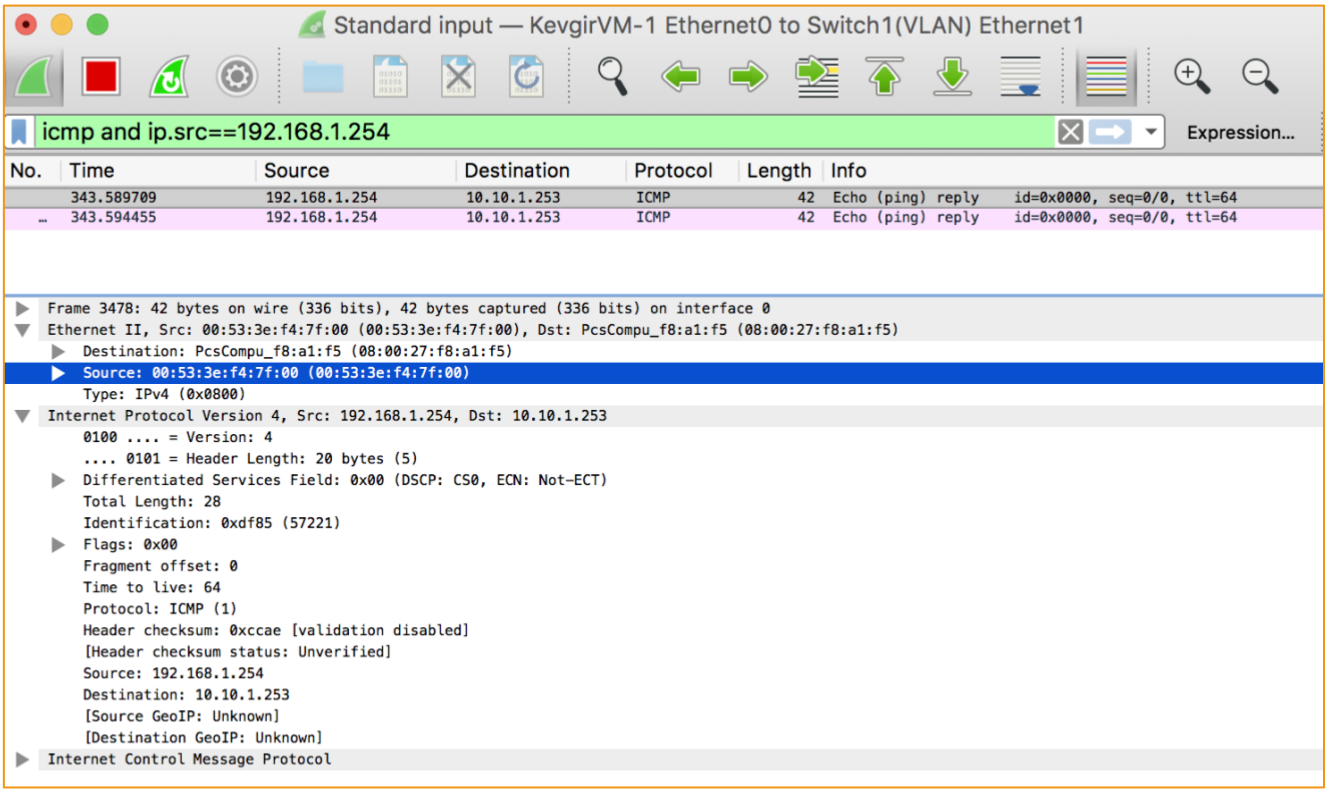
2.3.- Send the request. The student can use the option "count" to send a higher number of requests. By default, "*send*" only will send one packet. Note that in this example two packets are sent.



```
>>> request.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= icmp
  chksum= None
  src= 10.10.1.253
  dst= 192.168.1.254
  \options\
###[ ICMP ]###
     type= echo-request
     code= 0
     chksum= None
     id= 0x0
     seq= 0x0

>>> send(request,count=2,verbose=1)
..
Sent 2 packets.
```

Figure 39.Packet sent from Kali (M)

3.- Using the network sniffer (*Wireshark*) it is possible to see the **effect of the attack**. Note that 1) the router (A) receives a packet from the Kali Linux (M) but the IP of the packet is from the Kevgir VM (B), so the router replies to the Kegvir VM, that did not initiate the request.



Standard input — KevgirVM-1 Ethernet0 to Switch1(VLAN) Ethernet1
Expression...

icmp and ip.src==192.168.1.254

```
No.  Time          Source          Destination    Protocol  Length  Info
     343.589709    192.168.1.254   10.10.1.253    ICMP          42  Echo (ping) reply    id=0x0000, seq=0/0, ttl=64
…    343.594455    192.168.1.254   10.10.1.253    ICMP          42  Echo (ping) reply    id=0x0000, seq=0/0, ttl=64

▶ Frame 3478: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
▼ Ethernet II, Src: 00:53:3e:f4:7f:00 (00:53:3e:f4:7f:00), Dst: PcsCompu_f8:a1:f5 (08:00:27:f8:a1:f5)
   ▶ Destination: PcsCompu_f8:a1:f5 (08:00:27:f8:a1:f5)
   ▶ Source: 00:53:3e:f4:7f:00 (00:53:3e:f4:7f:00)
     Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 192.168.1.254, Dst: 10.10.1.253
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 28
     Identification: 0xdf85 (57221)
   ▶ Flags: 0x00
     Fragment offset: 0
     Time to live: 64
     Protocol: ICMP (1)
     Header checksum: 0xccae [validation disabled]
     [Header checksum status: Unverified]
     Source: 192.168.1.254
     Destination: 10.10.1.253
     [Source GeoIP: Unknown]
     [Destination GeoIP: Unknown]
▶ Internet Control Message Protocol
```

Figure 40. After *Scapy*: Kevgir VM receives two packets from the router

3.5 EXPLOITATION TOOLS

3.5.1 METASPLOIT

Metasploit is a very interesting exploitation framework. Kali Linux has the Community version installed, which is very complete. The professional version provides a nice web interface and some reporting tools which could help to build the reports about the findings. The tool provides a shell to perform the required operations with a wide range of modules available for attack. It is also possible to create **workspaces** to organize the attacks.

The core commands for *metasploit* can be obtained from different sources (https://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf).

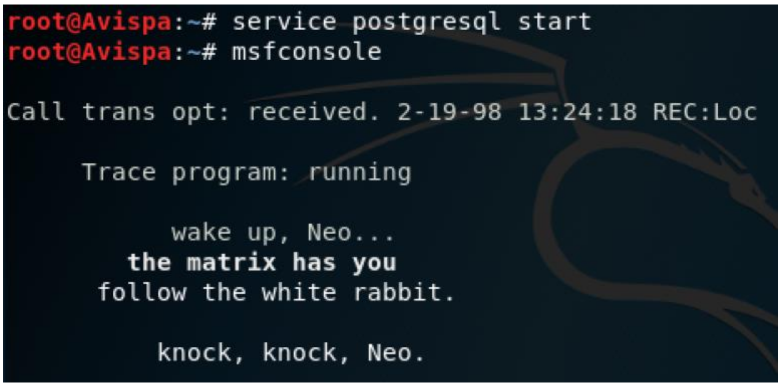
3.5.1.1 PRACTICAL EXAMPLE: TCP SYN FLOOD

The following example shows how to use *Metasploit* to perform a *TCP SYN Flood attack*. **Objective: it must be demonstrated that the target (a router) replies to the TCP SYN request.** Furthermore, the student should take into account the **steps for diagnosis recommended for the router** used in the example, that is, Mikrotik.

Steps:

1. The router (Mikrotik) will be the target. IP: 192.168.1.254.
    1.1. In order to check the **normal behaviour of the router before the attack,** the student should ***read*** the countermeasures section for this attack in Section 7.4.3, and check the tools for diagnosis.
    1.2. The sniffer should be connected:
        1.2.1. At some point between the router and the Kali, or in the Kali.
        1.2.2. Between the router Mikrotik and the Internet or the default gateway of the target router.

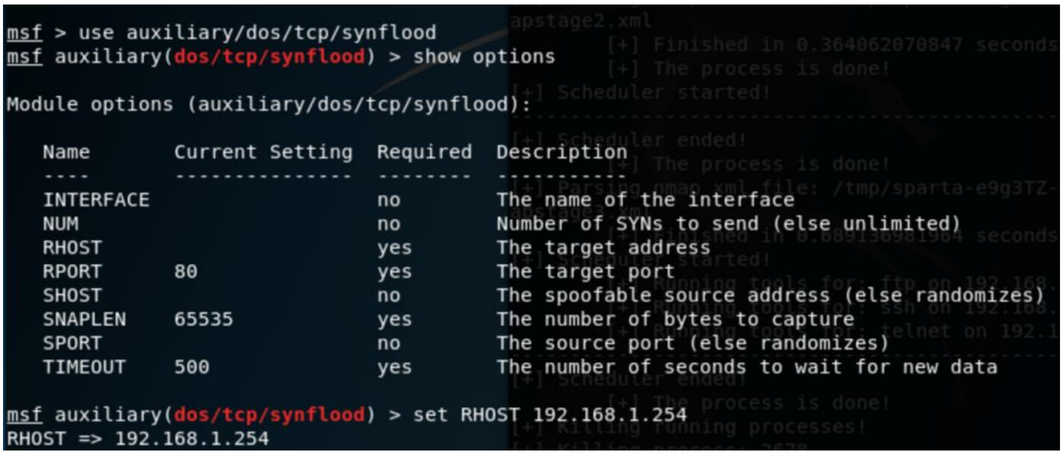
2. Kali will be the attacker's machine (IP 192.10.1.252). Therefore, metasploit will be used from Kali Linux. However, before this step, it is necessary to gather information about the open ports in mikrotik to be exploited (e.g. Sparta).



```
root@Avispa:~# service postgresql start
root@Avispa:~# msfconsole

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

           wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.
```

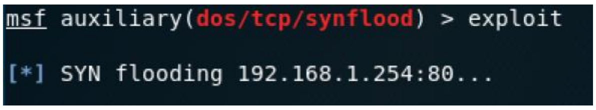
Figure 41. Executing *Metasploit*

3. Configure the parameters for the exploit, and launch it using the command "exploit".
    3.1. Note that the student must indicate the port of the service that is the target of the attack (80 by default), and the IP of the router Mikrotik where the service is running.



```
msf > use auxiliary/dos/tcp/synflood
msf auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   INTERFACE                   no        The name of the interface
   NUM                         no        Number of SYNs to send (else unlimited)
   RHOST                       yes       The target address
   RPORT      80               yes       The target port
   SHOST                       no        The spoofable source address (else randomizes)
   SNAPLEN    65535            yes       The number of bytes to capture
   SPORT                       no        The source port (else randomizes)
   TIMEOUT    500              yes       The number of seconds to wait for new data

msf auxiliary(dos/tcp/synflood) > set RHOST 192.168.1.254
RHOST => 192.168.1.254
```

Figure 42. Metasploit & *SYN flood*. Configuring the parameters



```
msf auxiliary(dos/tcp/synflood) > exploit

[*] SYN flooding 192.168.1.254:80...
```

Figure 43. SYN flood - exploit

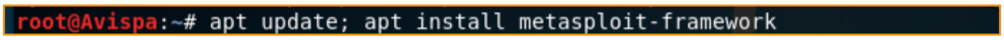
4. Check the results:
    4.1. Using the tools for diagnostics in the router (c.f. Section 7.4.3), check if the behaviour of the router is now different.
    4.2. Check the sniffers:
        4.2.1. In the sniffer between the Kali linux and the Mikrotik “SYN requests” must arise.
        4.2.2. In the sniffer between the Mikrotik router and the Internet “ACKs” should be present.
5. After a while, try to connect to the service in the port 80 to check if this is operative.

Note that, in order to satisfy the objective proposed, the target (Mikrotik) must reply to the TCP SYN. However, the **exploit will use random IPs in order to send the attack.** Therefore, the router will answer (ACK) to the Internet (the default gateway in our network).

The denial of service attack will be successful if we try to access the service of the attacked port without any success. However, for this proof of concept we reduce the objective to at least the router falling into the trap of responding to requests.

3.5.2 METASPLOIT FRAMEWORK

Some utilities can require the explicit installation of the metasploit framework. This can be installed using the following command.



```
root@Avispa:~# apt update; apt install metasploit-framework
```

Figure 44. Installing metasploit-framework

3.6 SNORT IN KALI

In order to make some tests with Snort, it can be useful install it in Kali Linux. Snort can be installed as follows:

```
# apt-get update
# apt-get install snort
```

To configure Snort, the student must follow the steps in Section 9 (Snort).

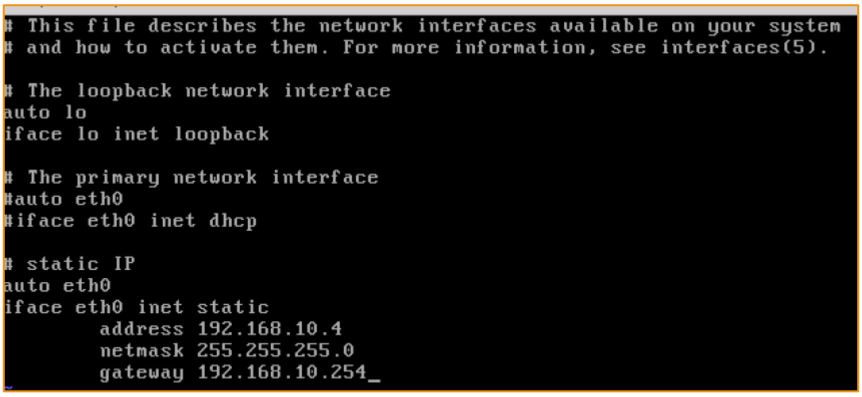
4 METASPLOITABLE 2 CONFIGURATION

This virtual machine has been downloaded from https://www.vulnhub.com/entry/metasploitable-2,29/#download

It can be opened with VMware Workstation Player, without additional configuration.

The login credentials are: msfadmin /msfadmin

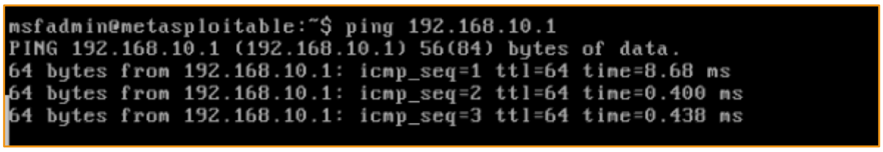
To set up a static IP, we must edit the file */etc/network/interfaces*. Open it as *superuser*, and include the lines shown in the next picture.



```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
#auto eth0
#iface eth0 inet dhcp

# static IP
auto eth0
iface eth0 inet static
        address 192.168.10.4
        netmask 255.255.255.0
        gateway 192.168.10.254_
```

Figure 45. Static IP - Metasploitable 2

Remember that the changes won't be effective until down and up of the interface *eth0*. Check the changes with "ifconfig". After this, it would be possible to ping to any other computer in the network.



```
msfadmin@metasploitable:~$ ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=8.68 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=0.400 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=64 time=0.438 ms
```

Figure 46. Ping from Metasploit 2 to PC-1 (simple network scenario)

4.1 CONNECT KALI 2 WITH METASPLOITABLE2

The aim is to connect Kali 2 with Metasploitable 2 in GNS3, using our simple network configuration. Note that, before this step, it is necessary to create a new template for metasploitable 2 in a similar way than the template for Kali.

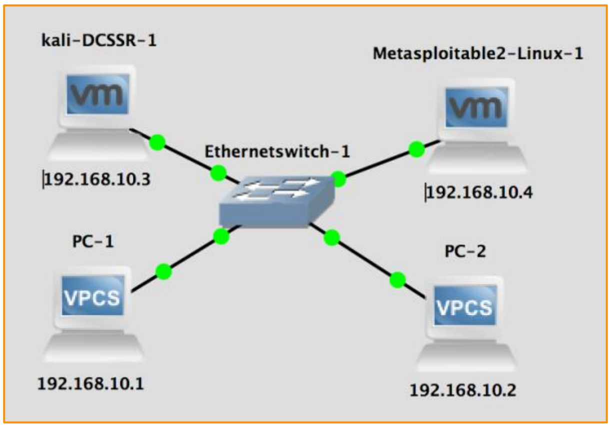
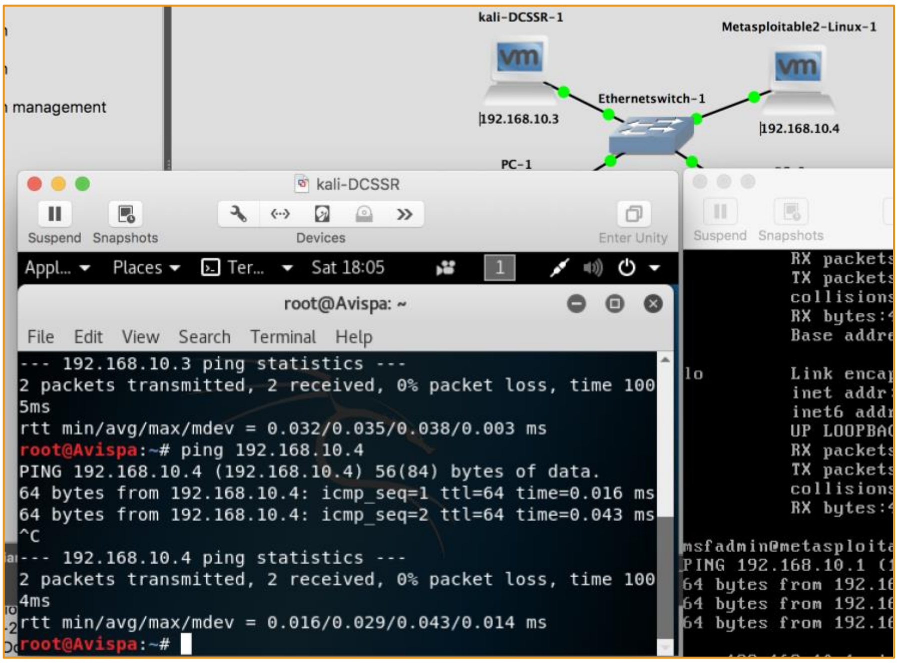


Figure 47. Kali and metasploitable 2 in the same network



```
--- 192.168.10.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 100
5ms
rtt min/avg/max/mdev = 0.032/0.035/0.038/0.003 ms
root@Avispa:~# ping 192.168.10.4
PING 192.168.10.4 (192.168.10.4) 56(84) bytes of data.
64 bytes from 192.168.10.4: icmp_seq=1 ttl=64 time=0.016 ms
64 bytes from 192.168.10.4: icmp_seq=2 ttl=64 time=0.043 ms
^C
--- 192.168.10.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 100
4ms
rtt min/avg/max/mdev = 0.016/0.029/0.043/0.014 ms
root@Avispa:~#
```

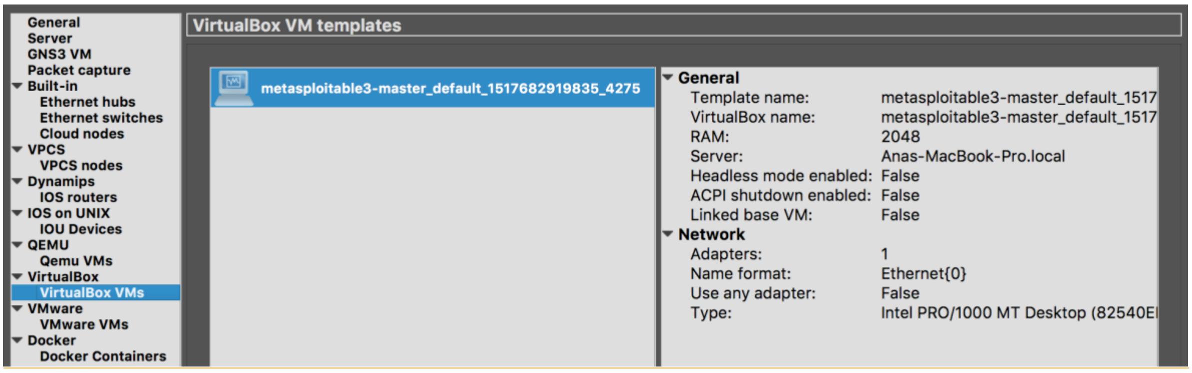
```
          RX packets
          TX packets
          collisions
          RX bytes:4
          Base addre

lo        Link encap
          inet addr
          inet6 addr
          UP LOOPBAC
          RX packets
          TX packets
          collisions
          RX bytes:4

msfadmin@metasploita
PING 192.168.10.1 (1
64 bytes from 192.16
64 bytes from 192.16
64 bytes from 192.16
```

Figure 48. Ping from Kali 2 to Metasploitable 2

5 METASPLOITABLE 3 CONFIGURATION

This virtual machine has been configured following the steps in the download page (build manually): https://github.com/rapid7/metasploitable3

The template for this virtual machine must be created in the options of VirtualBox.



VirtualBox VM templates

metasploitable3-master_default_1517682919835_4275

General

Template name:	metasploitable3-master_default_1517
VirtualBox name:	metasploitable3-master_default_1517
RAM:	2048
Server:	Anas-MacBook-Pro.local
Headless mode enabled:	False
ACPI shutdown enabled:	False
Linked base VM:	False

Network

Adapters:	1
Name format:	Ethernet{0}
Use any adapter:	False
Type:	Intel PRO/1000 MT Desktop (82540E

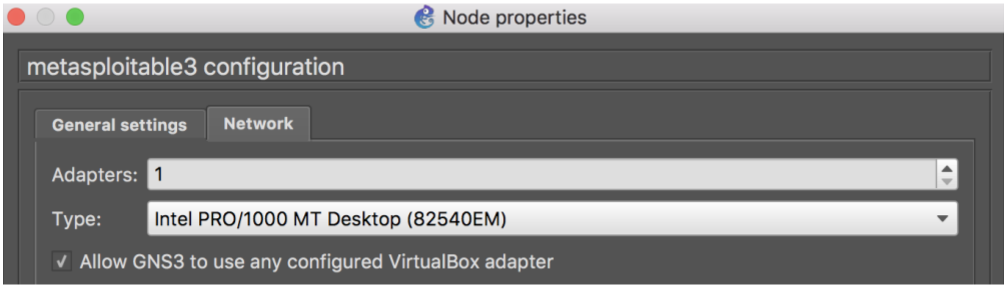
Figure 49. Template for Metasploitable3

5.1 TESTING METASPLOITABLE3

As in the previous case, it is necessary to check that: 1) it is possible to connect the template to any network element, 2) it is possible to modify the network interface to configure the network, and 3) the machine is effectively networked.

5.1.1 STEP1. CONNECT METASPLOITABLE3 TO A NETWORK

First, the student must edit the element Metasploitable3 to "allow GNS3 to use any configured VirtualBox adapter". This allows to connect the element "Metasploitable3" to the network.



Node properties

metasploitable3 configuration

Adapters: 1

Type: Intel PRO/1000 MT Desktop (82540EM)

☑ Allow GNS3 to use any configured VirtualBox adapter

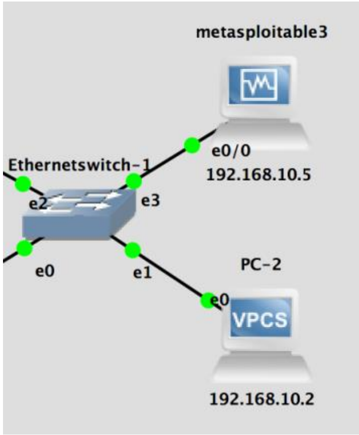


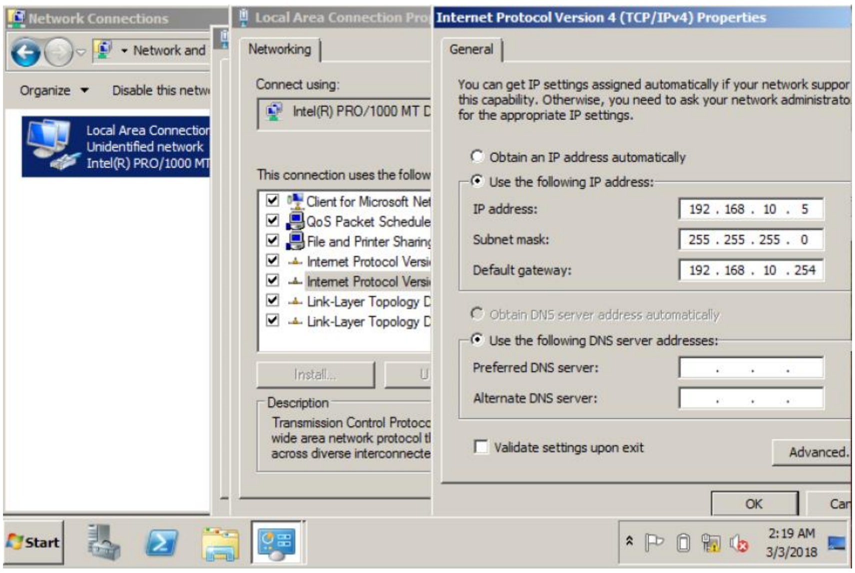
Figure 50. Metasploitable3 configuration in GNS3

5.1.2 STEP2. MODIFY THE NETWORK INTERFACE

The student must start the virtual machine using GNS3 (play).

The login credentials are: vagrant / vagrant

Unlike Metasploitable 2, this is a Windows virtual machine. Therefore, the configuration of the network interface must be done following the steps for a Windows machine: Change adapter settings, in the "Network and Sharing Center".



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network suppor this capability. Otherwise, you need to ask your network administrato for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 10 . 5
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 10 . 254

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	. . .
Alternate DNS server:	. . .

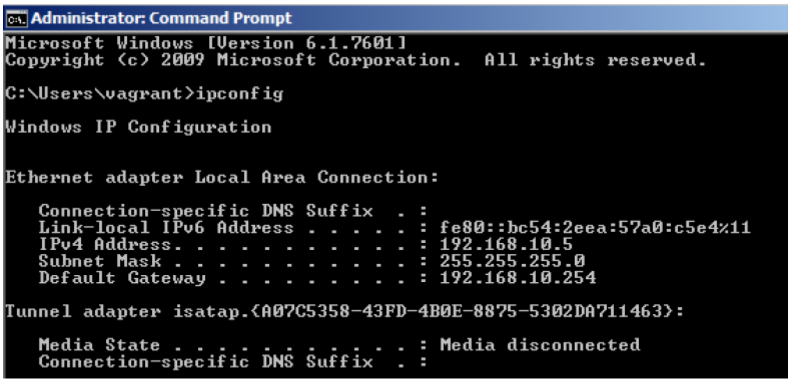
□ Validate settings upon exit

Advanced.

OK | Car

Figure 51. Metasploitable3 network configuration

The student must check the IP using the command line.



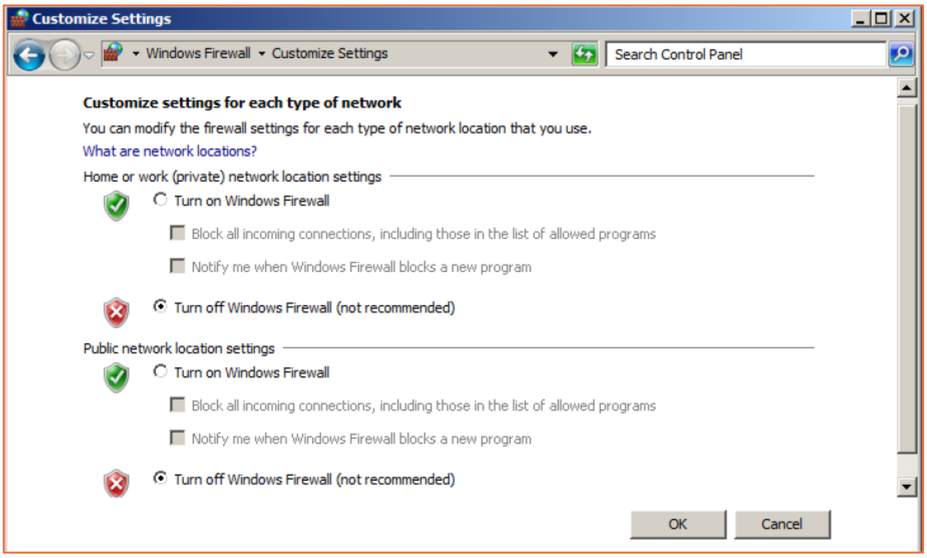
Administrator: Command Prompt

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\vagrant>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::bc54:2eea:57a0:c5e4%11
   IPv4 Address. . . . . . . . . . . : 192.168.10.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.254

Tunnel adapter isatap.{A07C5358-43FD-4B0E-8875-5302DA711463}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Figure 52. Ipconfig Metasploitable3

5.1.3 STEP3. METASPLOITABLE IN THE NETWORK

The student must disable the firewall in Metasploitable3.



Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

Home or work (private) network location settings

○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

□ Notify me when Windows Firewall blocks a new program

● Turn off Windows Firewall (not recommended)

Public network location settings

○ Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

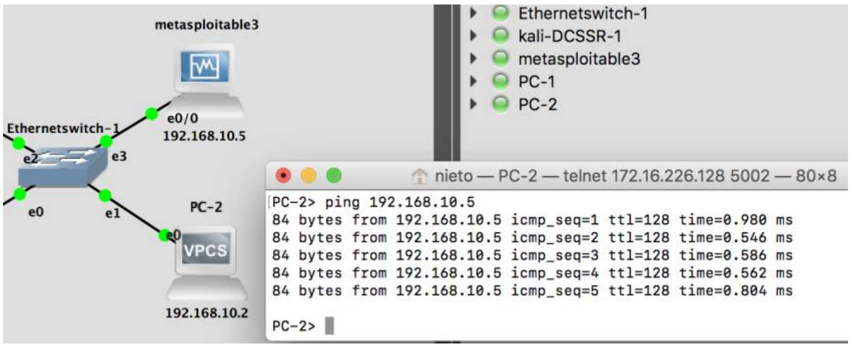
□ Notify me when Windows Firewall blocks a new program

● Turn off Windows Firewall (not recommended)

OK | Cancel

Figure 53. Turn off firewall in Metasploitable3

Afterwards, any other computer in the network should be able to ping to Metasploitable3.



```
PC-2> ping 192.168.10.5
84 bytes from 192.168.10.5 icmp_seq=1 ttl=128 time=0.980 ms
84 bytes from 192.168.10.5 icmp_seq=2 ttl=128 time=0.546 ms
84 bytes from 192.168.10.5 icmp_seq=3 ttl=128 time=0.586 ms
84 bytes from 192.168.10.5 icmp_seq=4 ttl=128 time=0.562 ms
84 bytes from 192.168.10.5 icmp_seq=5 ttl=128 time=0.804 ms

PC-2>
```

Figure 54. Ping from PC-2 to Metasploitable3

5.2 CONNECT KALI2 WITH METASPLOITABLE3

The student can add the element Metasploitable3 to the same network connecting Kali with Metasploitable2.

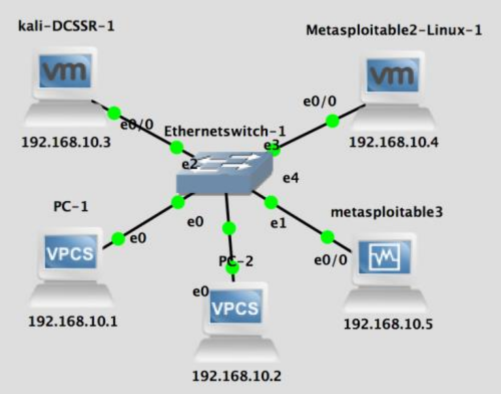
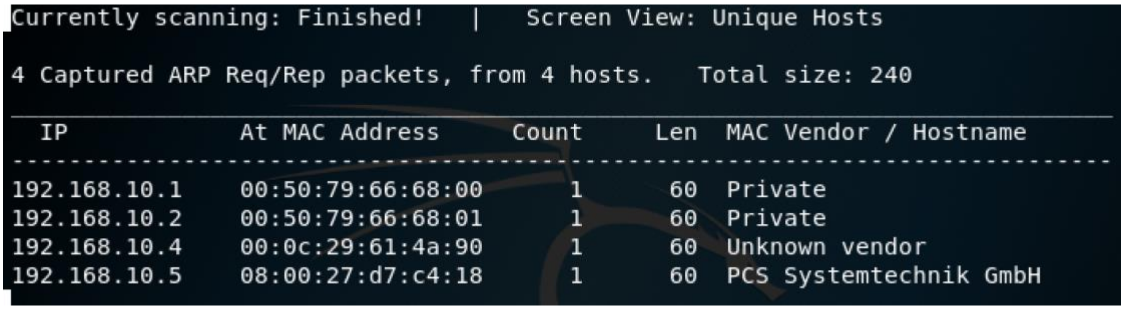


Figure 55. Kali and metasploitable3 in the same network

Using the network discovery tools in Kali Linux, it is possible to see all the PCs in the environment.



```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.10.1    00:50:79:66:68:00      1      60  Private
192.168.10.2    00:50:79:66:68:01      1      60  Private
192.168.10.4    00:0c:29:61:4a:90      1      60  Unknown vendor
192.168.10.5    08:00:27:d7:c4:18      1      60  PCS Systemtechnik GmbH
```

Figure 56. Output of “netdiscover -r 192.168.10.0/24” from Kali linux

6 VIRTUAL LAN (VLAN) CONFIGURATION

This is an example of VLAN configuration. Two VLANs are configured.

VLAN 10 is used to communicate PROF-1 and PROF-2, while VLAN 20 is used to communicate PHDS-1 and PHDS2.

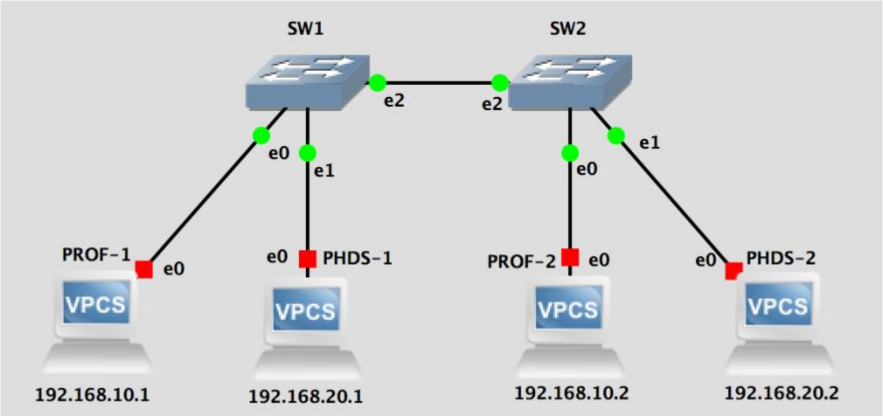
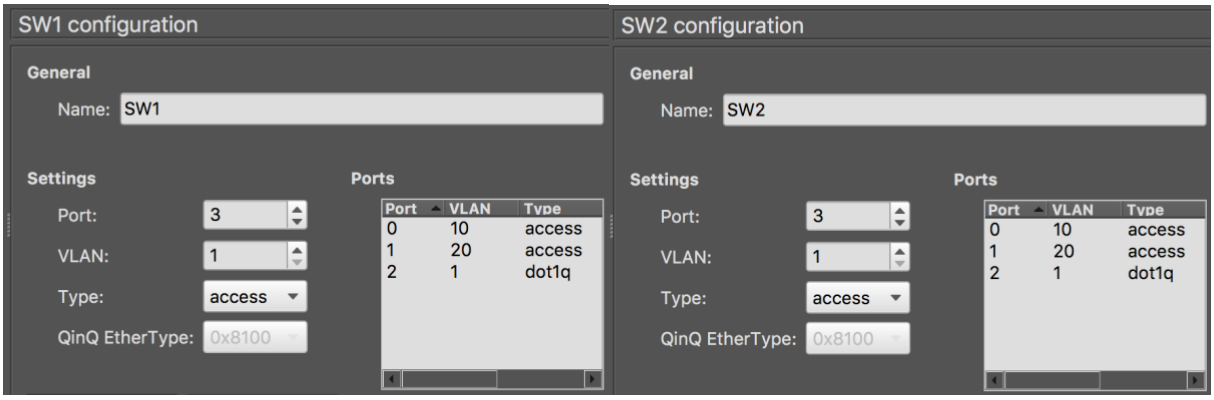


Figure 57. Basic VLAN

The following figure shows the configuration in the switches. *Dot1q* is for TRUNK.



SW1 configuration

General

Name: SW1

Settings

Port: 3

VLAN: 1

Type: access

QinQ EtherType: 0x8100

Ports

Port	VLAN	Type
0	10	access
1	20	access
2	1	dot1q

SW2 configuration

General

Name: SW2

Settings

Port: 3

VLAN: 1

Type: access

QinQ EtherType: 0x8100

Ports

Port	VLAN	Type
0	10	access
1	20	access
2	1	dot1q

Figure 58. Switches configuration for VLAN

In addition, the IPs for the VPCS must be configured (First test: Configure a basic Virtual network).

Note: try to make ping from 192.168.10.1 to 192.168.20.1. If the VLANs are well configured this will not be possible. You need a layer 3 switch to enable the communication between the VLANs or a router.

7 MIKROTIK (ROUTER)

The router *Mikrotik* is used in the laboratory. This section helps to learn the basic configuration to use this network element.

User: admin (there is no password).

7.1 DHCP-SERVER

The previous sections have shown how the clients must be configured to use DHCP. This service must be configured in the router, which is Mikrotik in our case.

The following are the instructions to configure the DHCP service in Mikrotik.

7.1.1 SIMPLE DHCP-SERVER

In this use case, we only have a network that needs a DHCP server. PC1 and PC2 will obtain their corresponding IP addresses using the router (mikrotik). PC1 and PC2 are in the same network, and *ether1* is the interface to provide the *dhcp* service.

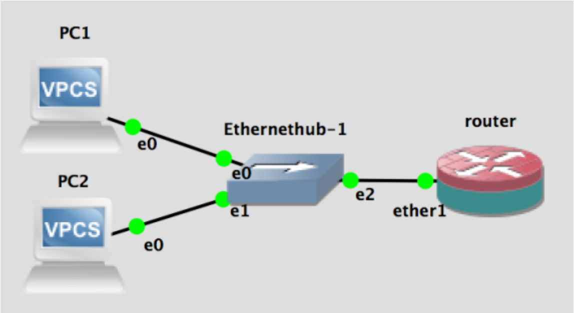
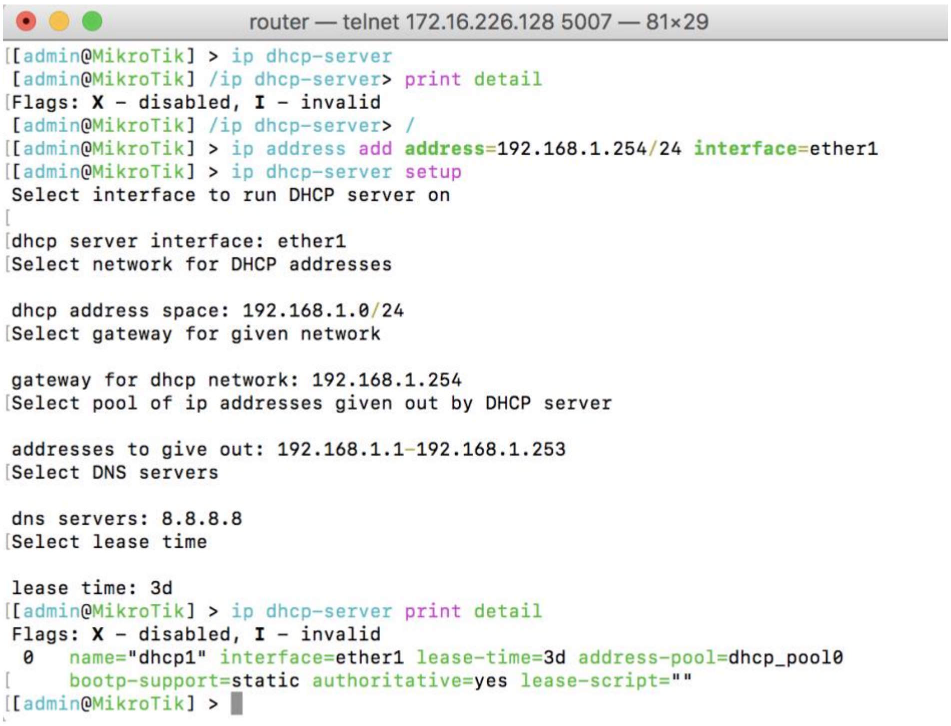


Figure 59. Network to test dhcp-server

The student must configure the router as follows:

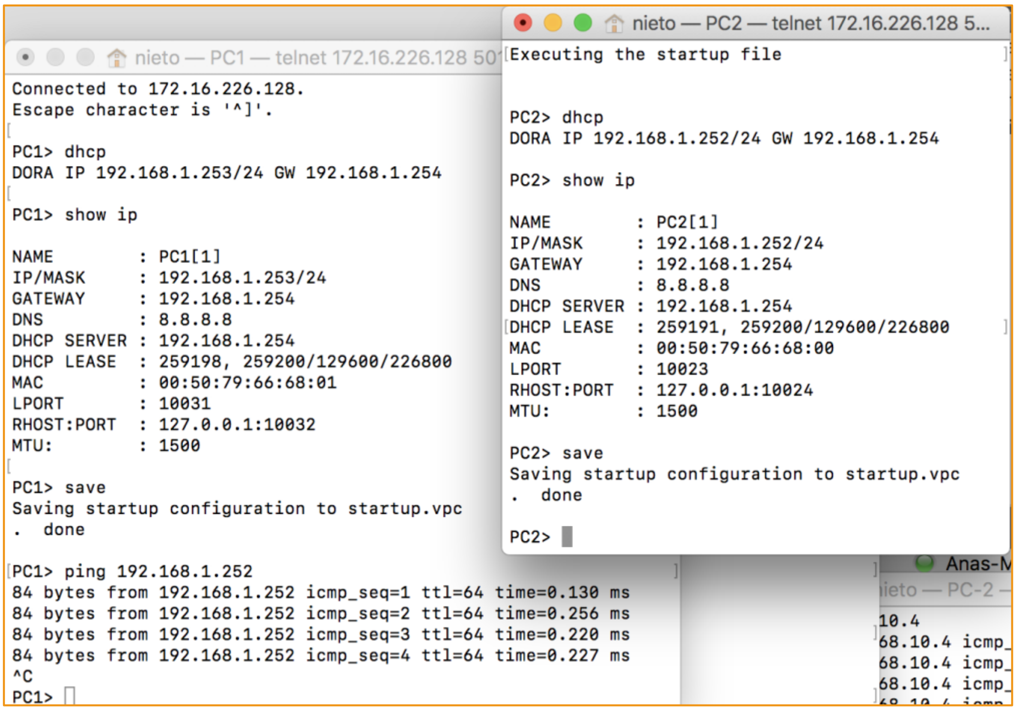


```
[admin@MikroTik] > ip dhcp-server
[admin@MikroTik] /ip dhcp-server> print detail
Flags: X - disabled, I - invalid
[admin@MikroTik] /ip dhcp-server> /
[admin@MikroTik] > ip address add address=192.168.1.254/24 interface=ether1
[admin@MikroTik] > ip dhcp-server setup
Select interface to run DHCP server on

dhcp server interface: ether1
Select network for DHCP addresses

dhcp address space: 192.168.1.0/24
Select gateway for given network

gateway for dhcp network: 192.168.1.254
Select pool of ip addresses given out by DHCP server

addresses to give out: 192.168.1.1-192.168.1.253
Select DNS servers

dns servers: 8.8.8.8
Select lease time

lease time: 3d
[admin@MikroTik] > ip dhcp-server print detail
Flags: X - disabled, I - invalid
 0   name="dhcp1" interface=ether1 lease-time=3d address-pool=dhcp_pool0
     bootp-support=static authoritative=yes lease-script=""
[admin@MikroTik] > █
```

Figure 60. Configuration of dhcp-server in ether1

Note that, in this case, the *dhcp-server* will provide IPs in the range 192.168.1.1-192.168.1.253. It is possible to modify this range in the case that the network has some static IPs.

The last step is to request the IP address, by using DHCP. The following picture shows an example using the VPCSs PC1 and PC2.


nieto — PC1 — telnet 172.16.226.128 50
nieto — PC2 — telnet 172.16.226.128 5...
Anas-M
ieto — PC-2 –

```
Connected to 172.16.226.128.
Escape character is '^]'.

PC1> dhcp
DORA IP 192.168.1.253/24 GW 192.168.1.254

PC1> show ip

NAME        : PC1[1]
IP/MASK     : 192.168.1.253/24
GATEWAY     : 192.168.1.254
DNS         : 8.8.8.8
DHCP SERVER : 192.168.1.254
DHCP LEASE  : 259198, 259200/129600/226800
MAC         : 00:50:79:66:68:01
LPORT       : 10031
RHOST:PORT  : 127.0.0.1:10032
MTU:        : 1500

PC1> save
Saving startup configuration to startup.vpc
.  done

PC1> ping 192.168.1.252
84 bytes from 192.168.1.252 icmp_seq=1 ttl=64 time=0.130 ms
84 bytes from 192.168.1.252 icmp_seq=2 ttl=64 time=0.256 ms
84 bytes from 192.168.1.252 icmp_seq=3 ttl=64 time=0.220 ms
84 bytes from 192.168.1.252 icmp_seq=4 ttl=64 time=0.227 ms
^C
PC1> 
```

```
Executing the startup file

PC2> dhcp
DORA IP 192.168.1.252/24 GW 192.168.1.254

PC2> show ip

NAME        : PC2[1]
IP/MASK     : 192.168.1.252/24
GATEWAY     : 192.168.1.254
DNS         : 8.8.8.8
DHCP SERVER : 192.168.1.254
DHCP LEASE  : 259191, 259200/129600/226800
MAC         : 00:50:79:66:68:00
LPORT       : 10023
RHOST:PORT  : 127.0.0.1:10024
MTU:        : 1500

PC2> save
Saving startup configuration to startup.vpc
.  done

PC2> 
```

```
10.4
68.10.4 icmp_
68.10.4 icmp_
68.10.4 icmp_
```

Figure 61. Get IP addresses using dhcp

7.1.2 CONFIGURING DHCP-SERVER FOR VLANS

In this use case, two different networks must be configured using the same network interface *ether1*. This is needed in case VLAN networks are present.

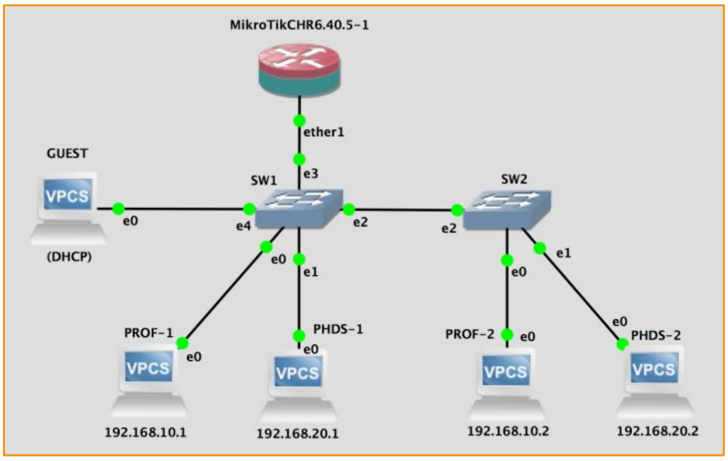


Figure 62. Multiple networks using the same network interface

The traffic from both *VLANs* will be received in the interface (ether1), the student will define two sub-interfaces for *ether1*:

[admin@MikroTik]> interface vlan add vlan-id=10 interface=ether1 name=ether1-vlan10

[admin@MikroTik]> interface vlan add vlan-id=20 interface=ether1 name=ether1-vlan20

Therefore, two IP addresses must be added:

```
[admin@MikroTik]> ip address add address=192.168.10.254/24 interface=ether1-vlan10

[admin@MikroTik]> ip address add address=192.168.20.254/24 interface=ether1-vlan20
```

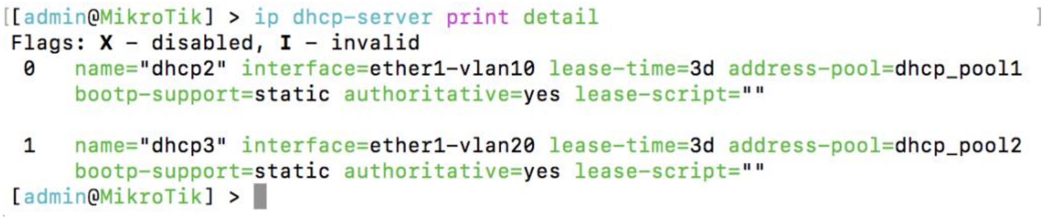
After the previous steps, the *DHCP-server* must be configured (ip dhcp-server setup, Figure 60. Configuration of dhcp-server in ether1). The first one using the interface *ether1-vlan10*, and the second one using the interface *ether1-vlan20*.

7.1.2.1 MORE INFORMATION

More information about DHCP-server in Mikrotik: https://wiki.mikrotik.com/wiki/Manual:IP/DHCP_Server

More information about VLAN in Mikrotik: https://wiki.mikrotik.com/wiki/Manual:Interface/VLAN

The following figure shows the configuration for both interfaces using two different pools.



```
[[admin@MikroTik] > ip dhcp-server print detail                       ]
 Flags: X - disabled, I - invalid
  0    name="dhcp2" interface=ether1-vlan10 lease-time=3d address-pool=dhcp_pool1
       bootp-support=static authoritative=yes lease-script=""

  1    name="dhcp3" interface=ether1-vlan20 lease-time=3d address-pool=dhcp_pool2
       bootp-support=static authoritative=yes lease-script=""
 [admin@MikroTik] >
```

Figure 63. DHCP-server print detail (VLAN interfaces)

7.2 CONNECT TWO ROUTERS

This can be useful to configure an internal router using a static IP (192.168.1.253) to connect with the external router (IP 192.168.1.254). Additional information can be found in this link for a simple network.

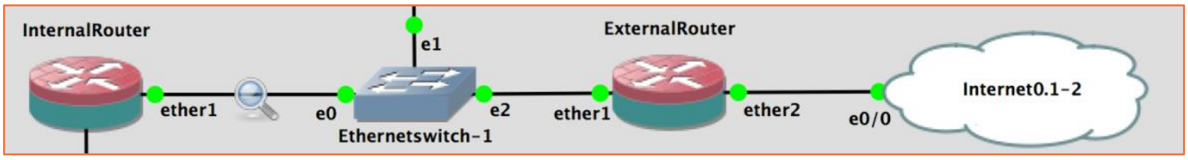


Figure 64 Simple configuration to connect InternalRouter to ExternalRouter

Assuming that **ExternalRouter is already configured**, the following steps are required to configure InternalRouter:

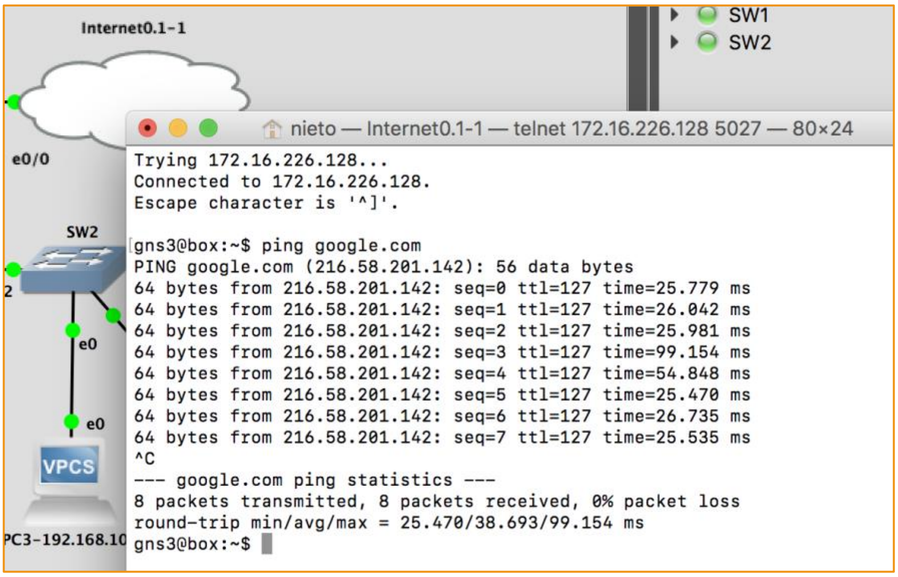
1. Configure the static IP for ether1:
```
[admin@MikroTik] /ip address> add address=192.168.1.253/30 interface=ether1
```
2. Add the gateway for InternalRouter: ExternalRouter
```
[admin@MikroTik] > ip route add gateway=192.168.1.254
```
3. Add the DNS
```
[[admin@MikroTik] > ip dns set servers=8.8.8.8 allow-remote-requests=yes
```
4. Check the connection
```
[[admin@MikroTik] > ping google.com
  SEQ HOST                                      SIZE TTL TIME  STATUS
    0 172.217.16.238                              56 125 15ms
    1 172.217.16.238                              56 125 14ms
    sent=2 received=2 packet-loss=0% min-rtt=14ms avg-rtt=14ms max-rtt=15ms
```

7.3 CONFIGURE THE ACCESS TO THE INTERNET IN GNS3

The student needs the following (find the links in the virtual campus):

- The Internet appliance for GNS3.
- The appliance for Mikrotik (router).

The element "Internet" is configured by default. You can test it with a ping to google.



```
Trying 172.16.226.128...
Connected to 172.16.226.128.
Escape character is '^]'.

gns3@box:~$ ping google.com
PING google.com (216.58.201.142): 56 data bytes
64 bytes from 216.58.201.142: seq=0 ttl=127 time=25.779 ms
64 bytes from 216.58.201.142: seq=1 ttl=127 time=26.042 ms
64 bytes from 216.58.201.142: seq=2 ttl=127 time=25.981 ms
64 bytes from 216.58.201.142: seq=3 ttl=127 time=99.154 ms
64 bytes from 216.58.201.142: seq=4 ttl=127 time=54.848 ms
64 bytes from 216.58.201.142: seq=5 ttl=127 time=25.470 ms
64 bytes from 216.58.201.142: seq=6 ttl=127 time=26.735 ms
64 bytes from 216.58.201.142: seq=7 ttl=127 time=25.535 ms
^C
--- google.com ping statistics ---
8 packets transmitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 25.470/38.693/99.154 ms
gns3@box:~$
```

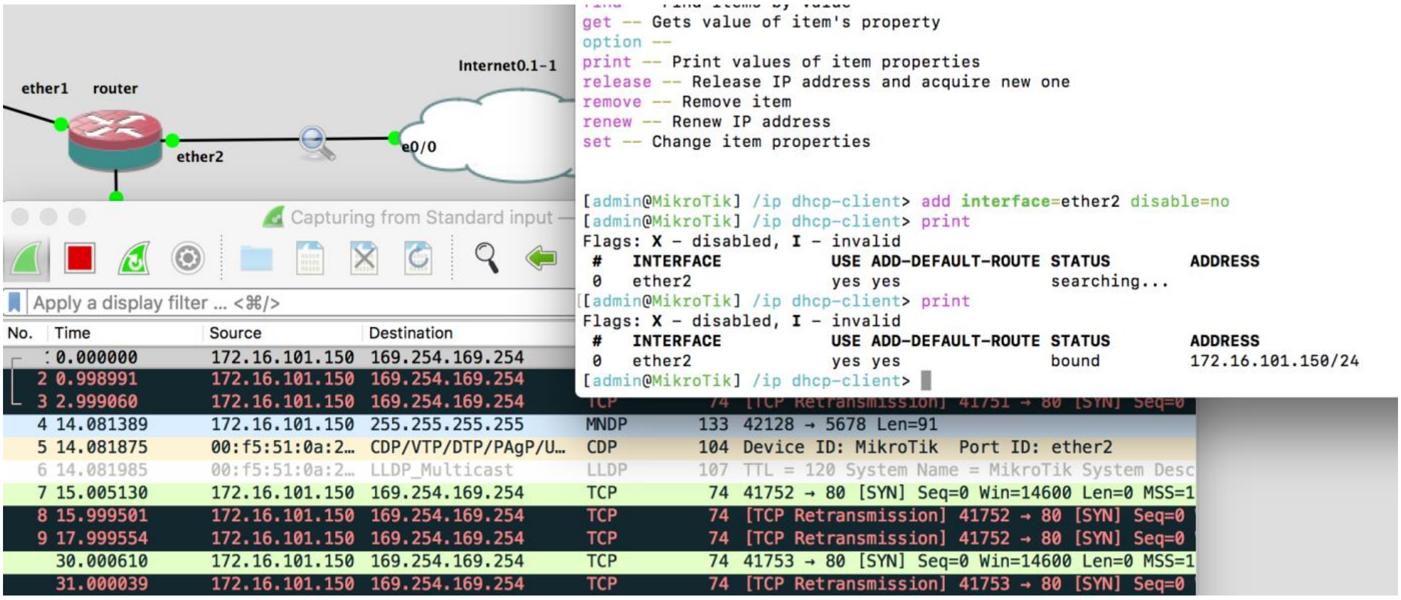
Figure 65. Ping to google.com from the element "Internet"

Therefore, in the following steps the configuration of the router is needed.

7.3.1 STEP 1: DHCP-CLIENT FOR MIKROTIK

The student must configure the *dhcp-client* for the *mikrotik* router using the command shown in the picture below: "ip dhcp-client add interface=[name of the interface] disabled=no".

It can be observed how the system will assign an IP address to *ether2*.

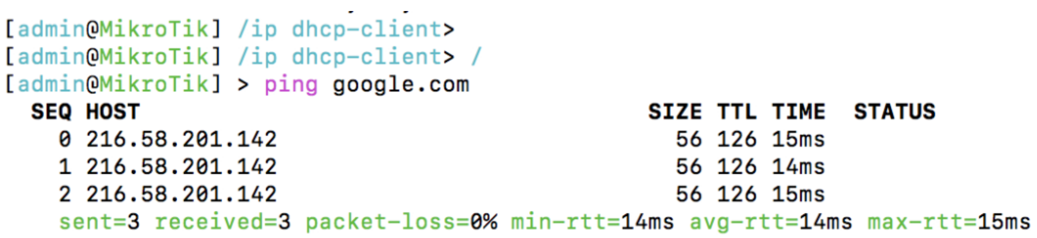

ether1
router
ether2
Internet0.1-1
e0/0
Capturing from Standard input
Apply a display filter ... <⌘/>

```
get -- Gets value of item's property
option --
print -- Print values of item properties
release -- Release IP address and acquire new one
remove -- Remove item
renew -- Renew IP address
set -- Change item properties


[admin@MikroTik] /ip dhcp-client> add interface=ether2 disable=no
[admin@MikroTik] /ip dhcp-client> print
Flags: X - disabled, I - invalid
 #   INTERFACE            USE ADD-DEFAULT-ROUTE STATUS        ADDRESS
 0   ether2               yes yes               searching...
[admin@MikroTik] /ip dhcp-client> print
Flags: X - disabled, I - invalid
 #   INTERFACE            USE ADD-DEFAULT-ROUTE STATUS        ADDRESS
 0   ether2               yes yes               bound         172.16.101.150/24
[admin@MikroTik] /ip dhcp-client>
```

```
No. Time        Source          Destination
  : 0.000000    172.16.101.150  169.254.169.254
  2 0.998991    172.16.101.150  169.254.169.254
  3 2.999060    172.16.101.150  169.254.169.254
  4 14.081389   172.16.101.150  255.255.255.255  MNDP  133 42128 → 5678 Len=91
  5 14.081875   00:f5:51:0a:2…  CDP/VTP/DTP/PAgP/U…  CDP  104 Device ID: MikroTik  Port ID: ether2
  6 14.081985   00:f5:51:0a:2…  LLDP_Multicast   LLDP  107 TTL = 120 System Name = MikroTik System Desc
  7 15.005130   172.16.101.150  169.254.169.254  TCP    74 41752 → 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1
  8 15.999501   172.16.101.150  169.254.169.254  TCP    74 [TCP Retransmission] 41752 → 80 [SYN] Seq=0
  9 17.999554   172.16.101.150  169.254.169.254  TCP    74 [TCP Retransmission] 41752 → 80 [SYN] Seq=0
    30.000610   172.16.101.150  169.254.169.254  TCP    74 41753 → 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1
    31.000039   172.16.101.150  169.254.169.254  TCP    74 [TCP Retransmission] 41753 → 80 [SYN] Seq=0
```

Figure 66. Configuring DHCP-client in Mikrotik

Now, it would be possible to access to Internet from the *Mikrotik* router:



```
[admin@MikroTik] /ip dhcp-client>
[admin@MikroTik] /ip dhcp-client> /
[admin@MikroTik] > ping google.com
  SEQ HOST                                     SIZE TTL TIME   STATUS
    0 216.58.201.142                             56 126 15ms
    1 216.58.201.142                             56 126 14ms
    2 216.58.201.142                             56 126 15ms
    sent=3 received=3 packet-loss=0% min-rtt=14ms avg-rtt=14ms max-rtt=15ms
```

Figure 67 Ping to google.com from Mikrotik

7.3.2 STEP 2: CONFIGURE NETWORK ADDRESSS TRANSLATION (NAT) IN MIKROTIK

This step is needed to connect to the rest of devices in the network to the Internet. For this, the Network Address Translation (NAT) must be configured in the router in order to map private IP addresses to public directions.

The instructions to configure NAT can be found in https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/NAT. In particular, the options to configure NAT are in "ip firewall nat". Here, we consider the following scenario, where the interface *ether1* in Mikrotik is used by two VLANs.

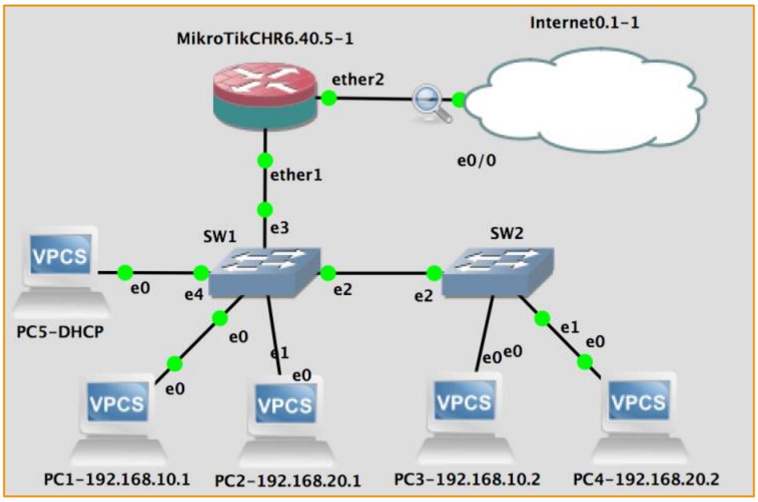
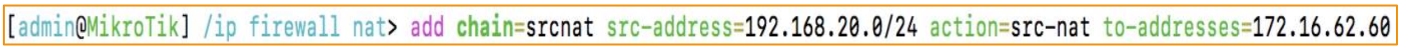


Figure 68. Network connected to the Internet

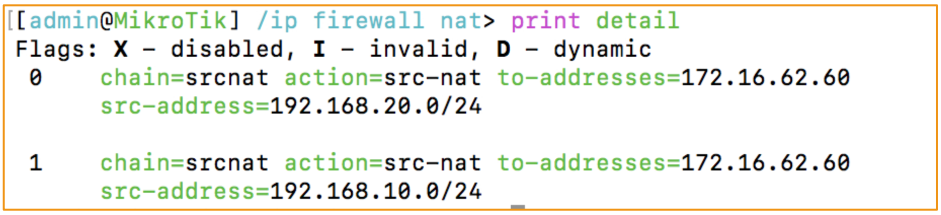
Therefore, two instructions must be added, one for each *VLAN*. The following picture shows an example for the *VLAN 20*; note that a similar expression will be required for the *VLAN 10*:



```
[admin@MikroTik] /ip firewall nat> add chain=srcnat src-address=192.168.20.0/24 action=src-nat to-addresses=172.16.62.60
```

Figure 69. Configuring NAT for VLAN 20

Finally, the following picture shows the result after the configuration of NAT.

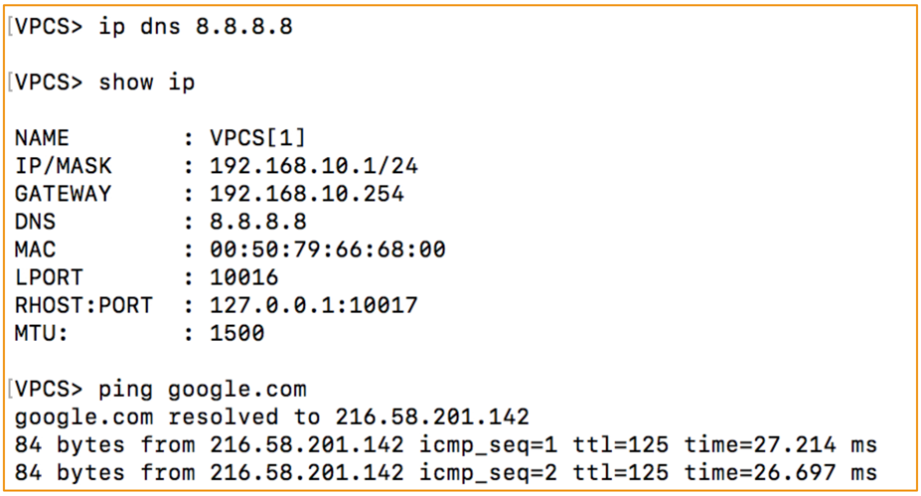


```
[admin@MikroTik] /ip firewall nat> print detail
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=srcnat action=src-nat to-addresses=172.16.62.60
      src-address=192.168.20.0/24

 1    chain=srcnat action=src-nat to-addresses=172.16.62.60
      src-address=192.168.10.0/24
```

Figure 70. NAT configuration in Mikrotik

7.3.3 STEP 3: CONFIGURE THE DNS IN THE VPCS

After the previous step, it will be possible to make a ping to *google.com* from any VPCS / host. You must ensure that the DNS is correct. You can use, for example, *8.8.8.8*.



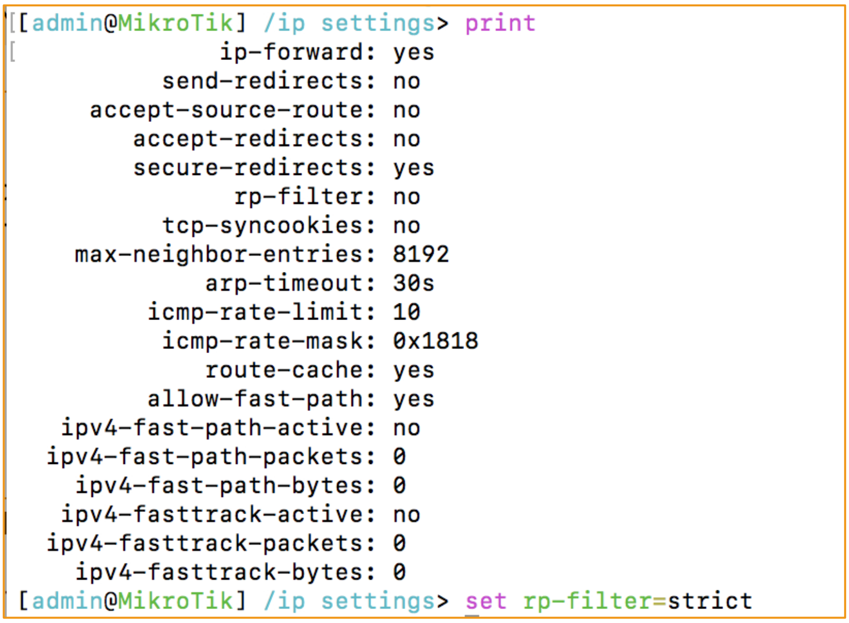
```
VPCS> ip dns 8.8.8.8

VPCS> show ip

NAME        : VPCS[1]
IP/MASK     : 192.168.10.1/24
GATEWAY     : 192.168.10.254
DNS         : 8.8.8.8
MAC         : 00:50:79:66:68:00
LPORT       : 10016
RHOST:PORT  : 127.0.0.1:10017
MTU:        : 1500

VPCS> ping google.com
google.com resolved to 216.58.201.142
84 bytes from 216.58.201.142 icmp_seq=1 ttl=125 time=27.214 ms
84 bytes from 216.58.201.142 icmp_seq=2 ttl=125 time=26.697 ms
```

Figure 71. Ping to *google.com* from a VPCS

7.4 COUNTERMEASURES TO PREVENT ATTACKS

7.4.1 IP SPOOFING

To avoid IP spoofing, it is recommended to enable *strict mode* in the feature **Reverse Path Filtering** (RPF). This feature is enabled/disabled in "ip settings" as follows (https://wiki.mikrotik.com/wiki/Manual:IP/Settings):



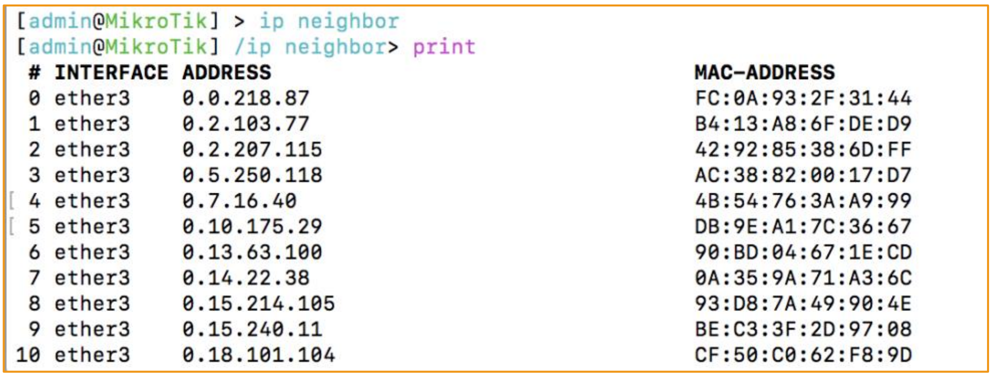
```
[admin@MikroTik] /ip settings> print
              ip-forward: yes
          send-redirects: no
     accept-source-route: no
        accept-redirects: no
        secure-redirects: yes
               rp-filter: no
          tcp-syncookies: no
    max-neighbor-entries: 8192
             arp-timeout: 30s
         icmp-rate-limit: 10
          icmp-rate-mask: 0x1818
             route-cache: yes
         allow-fast-path: yes
   ipv4-fast-path-active: no
  ipv4-fast-path-packets: 0
    ipv4-fast-path-bytes: 0
   ipv4-fasttrack-active: no
  ipv4-fasttrack-packets: 0
    ipv4-fasttrack-bytes: 0
[admin@MikroTik] /ip settings> set rp-filter=strict
```

Figure 72. Strict RPF to avoid IP spoofing

This also avoids some DDoS attacks from an internal LAN subnet.

7.4.2 CDP FLOODING ATTACKS

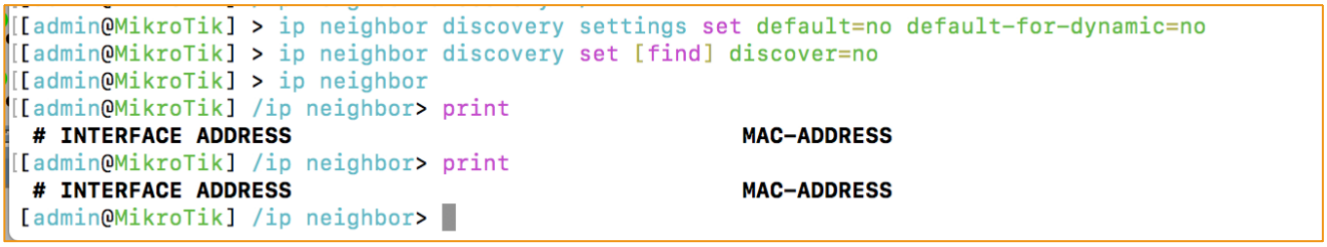
The Cisco Discovery Protocol (CDP) is a proprietary protocol that all Cisco devices can use by default. "*MikroTik Neighbor Discovery Protocol (MNDP) allows to find other devices compatible with MNDP, CDP, or LLDP (Link Layer Discovery Protocol) in layer 2 broadcast domain*" (https://wiki.mikrotik.com/wiki/Manual:IP/Neighbor_discovery). It is possible to check that the router MikroTik can be affected by this attack when it is launched from Kali Linux.



```
[admin@MikroTik] > ip neighbor
[admin@MikroTik] /ip neighbor> print
 # INTERFACE ADDRESS                                 MAC-ADDRESS
 0 ether3    0.0.218.87                              FC:0A:93:2F:31:44
 1 ether3    0.2.103.77                              B4:13:A8:6F:DE:D9
 2 ether3    0.2.207.115                             42:92:85:38:6D:FF
 3 ether3    0.5.250.118                             AC:38:82:00:17:D7
 4 ether3    0.7.16.40                               4B:54:76:3A:A9:99
 5 ether3    0.10.175.29                             DB:9E:A1:7C:36:67
 6 ether3    0.13.63.100                             90:BD:04:67:1E:CD
 7 ether3    0.14.22.38                              0A:35:9A:71:A3:6C
 8 ether3    0.15.214.105                            93:D8:7A:49:90:4E
 9 ether3    0.15.240.11                             BE:C3:3F:2D:97:08
10 ether3    0.18.101.104                            CF:50:C0:62:F8:9D
```

Figure 73. Router MikroTik after a CDP flooding attack

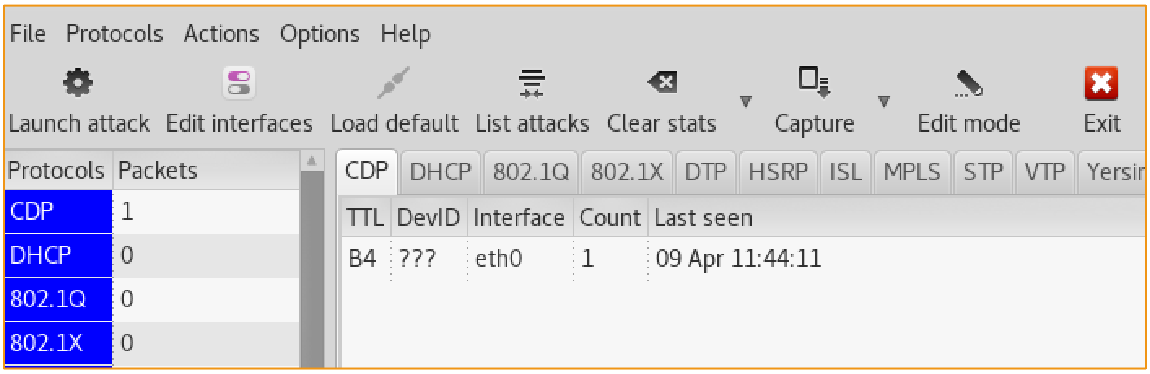
To avoid this attack, the student must **disable neighbour discovery**. This can be done in MikroTik using the following two instructions:



```
[admin@MikroTik] > ip neighbor discovery settings set default=no default-for-dynamic=no
[admin@MikroTik] > ip neighbor discovery set [find] discover=no
[admin@MikroTik] > ip neighbor
[admin@MikroTik] /ip neighbor> print
 # INTERFACE ADDRESS                          MAC-ADDRESS
[admin@MikroTik] /ip neighbor> print
 # INTERFACE ADDRESS                          MAC-ADDRESS
[admin@MikroTik] /ip neighbor> 
```

Figure 74. Avoiding CDP flooding attack (and discovery) in MikroTik

Figure 74 shows two prints. The first one is before launching the CDP flooding attack from Yersinia. The second one is after launching the attack. In addition, Figure 75 shows the window for Yersinia when the attack is executed. Note that this is quite different from an effective attack (c.f. Figure 32).



Protocols	Packets
CDP	1
DHCP	0
802.1Q	0
802.1X	0

TTL	DevID	Interface	Count	Last seen
B4	???	eth0	1	09 Apr 11:44:11

Figure 75. CDP flooding attack from Yersinia (fail)

7.4.3 TCP SYN FLOODING

This information is in the official website of mikrotik: https://wiki.mikrotik.com/wiki/DoS_attack_protection. Additional information about the the properties in: https://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Filter

Diagnose:

Question for diagnosis of SYN flood	How to check it in Mikrotik
Are there too many connections with syn-sent state present?	/ip firewall connection print
Are there too many packets per second going through any interface?	/interface monitor-traffic ether3
Is CPU usage 100%?	/system resource monitor
Are there too many suspicious connections?	/tool torch

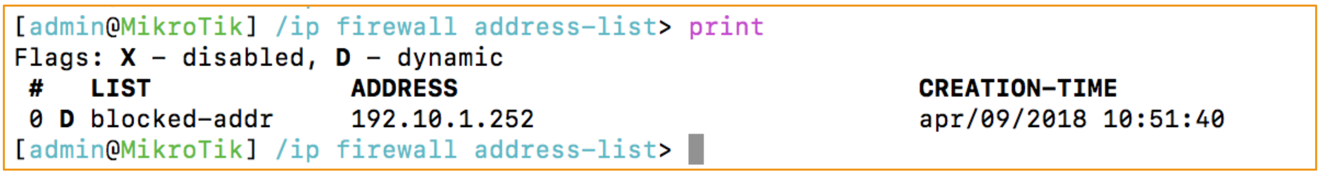
Protection:

Alternatives for protection	How to configure Mikrotik
Limit incoming connections. An IP address with too many connections can be added to a 'black-list' type address list for further blocking.	/ip firewall filter add chain=input protocol=tcp connection-limit=3,32 \ action=add-src-to-address-list address-list=blocked-addr address-list-timeout=1d
Action tarpit. Instead of simply dropping attacker's packets (with 'action=drop') router can capture and hold connections, and with a powerful enough router it can slow the attacker down.	/ip firewall filter add chain=input protocol=tcp src-address-list=blocked-addr \ connection-limit=3,32 action=tarpit

SYN filtering. Some advanced filtering can be applied to tcp packet state.	/ip firewall filter add chain=forward protocol=tcp tcp-flags=syn connection-state=new \
	action=jump jump-target=SYN-Protect comment="SYN Flood protect" disabled=yes
	/ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn limit=400,5 connection-state=new \
	action=accept comment="" disabled=no
	/ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn connection-state=new \
	action=drop comment="" disabled=no

SYN cookies. Technique use to resist SYN flood attacks. Allows a server to avoid dropping connections when the SYN queue fills up. Instead, the server behaves as if the SYN queue had been enlarged.	For v6.x: /ip settings set tcp-syncookies=yes For older RouterOS versions: /ip firewall connection tracking set tcp-syncookie=yes

For example, using the first alternative, the source of the ***TCP SYN flooding attack*** is added to a black-list as shown in the following figure.



```
[admin@MikroTik] /ip firewall address-list> print
Flags: X - disabled, D - dynamic
 #   LIST              ADDRESS                                     CREATION-TIME
 0 D blocked-addr      192.10.1.252                                apr/09/2018 10:51:40
[admin@MikroTik] /ip firewall address-list>
```

Figure 76. Black list created for MikroTik

8 PFSENSE (NETWORK FIREWALL)

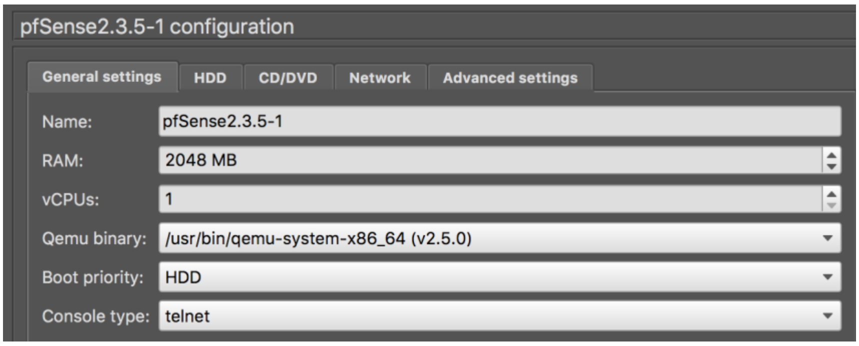
"The pfSense project is a free network firewall distribution, based on the FreeBSD operating system with a custom kernel and including third party free software packages for additional functionality. pfSense software, with the help of the package system, is able to provide the same functionality or more of common commercial firewalls, without any of the artificial limitations. It has successfully replaced every big name commercial firewall you can imagine in numerous installations around the world, including Check Point, Cisco PIX, Cisco ASA, Juniper, Sonicwall, Netgear, Watchguard, Astaro, and more.". The student can find a list of characteristics of this firewall in the following link: https://www.pfsense.org/about-pfsense/features.html

User: **admin**, Password: **pfsense**.

The steps in this guide are for pfSense v.2.3.5. New versions such as 2.4.4 requires additional steps not included here, mainly for the initial installation of the software in the pfSense.

8.1 REQUIREMENTS FOR PFSENSE

The first step is to check the requirements in the computer. Once installed, pfSense will require 2048MB of RAM. It is very important to ensure that it will be viable to have this memory to emulate pfSense. If pfSense will be linked to the GNS3 VM (recommended), then, ensure enough memory in the GNS3 VM to run pfSense.



pfSense2.3.5-1 configuration

Name: pfSense2.3.5-1

RAM: 2048 MB

vCPUs: 1

Qemu binary: /usr/bin/qemu-system-x86_64 (v2.5.0)

Boot priority: HDD

Console type: telnet

Figure 77. pfSense requirements in the computer

8.2 INSTALLING PFSENSE

The appliance for pfSense is not installed in the laboratory. However, the student can find this appliance listed in GNS3:

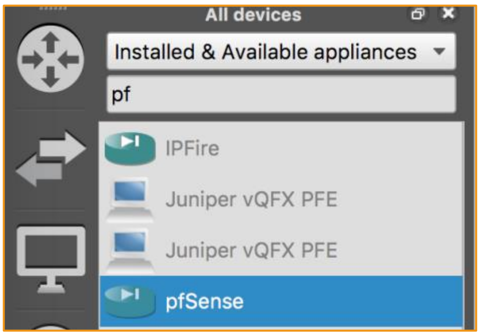
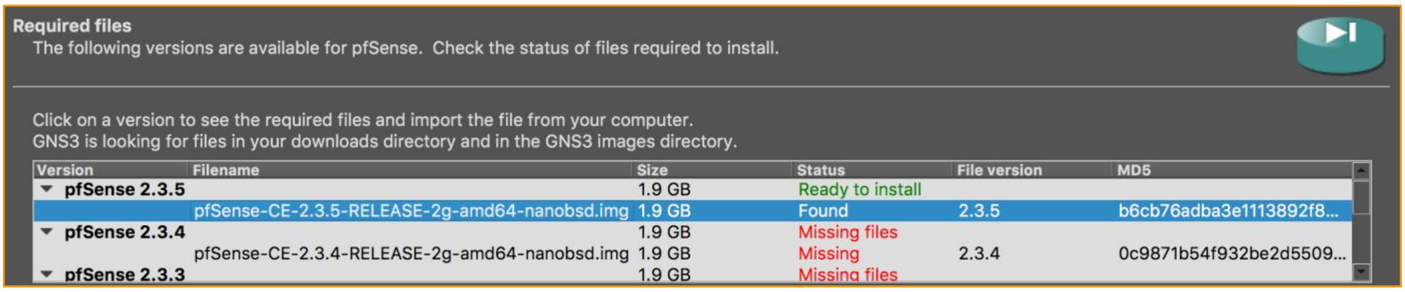


Figure 78. pfSense in "available appliances"

If the student selects the appliance, a window appears to install this appliance. In the next figure, the additional file to install this appliance is shown. This can be downloaded from: https://docs.gns3.com/appliances/pfsense.html#appliance_supported



Required files
The following versions are available for pfSense. Check the status of files required to install.

Click on a version to see the required files and import the file from your computer.
GNS3 is looking for files in your downloads directory and in the GNS3 images directory.

Version	Filename	Size	Status	File version	MD5
▼ pfSense 2.3.5		1.9 GB	Ready to install		
	pfSense-CE-2.3.5-RELEASE-2g-amd64-nanobsd.img	1.9 GB	Found	2.3.5	b6cb76adba3e1113892f8...
▼ pfSense 2.3.4		1.9 GB	Missing files		
	pfSense-CE-2.3.4-RELEASE-2g-amd64-nanobsd.img	1.9 GB	Missing	2.3.4	0c9871b54f932be2d5509...
▼ pfSense 2.3.3		1.9 GB	Missing files		

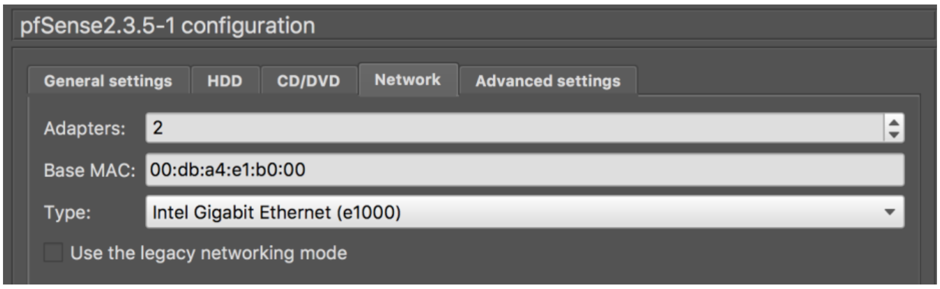
Figure 79. Files required to install pfSense

Therefore, the student must:

1) Download the file required to install pfSense (.img)
2) Install the pfSense appliance for GNS3

8.3 STARTING WITH PFSENSE

The pfSense network firewall has several network adapters defined by default. The student must limit these to two: one for the LAN and another for the WAN. Otherwise, problems may occur during the initial configuration.



pfSense2.3.5-1 configuration

Adapters: 2
Base MAC: 00:db:a4:e1:b0:00
Type: Intel Gigabit Ethernet (e1000)
□ Use the legacy networking mode

Figure 80. Network adapters pfSense

Then, the firewall must be connected to the elements in the network as follows:

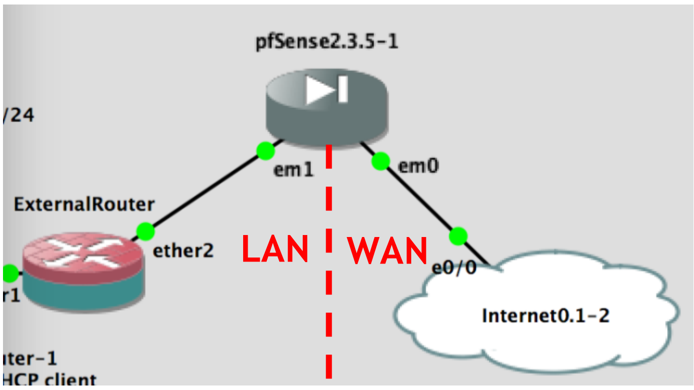
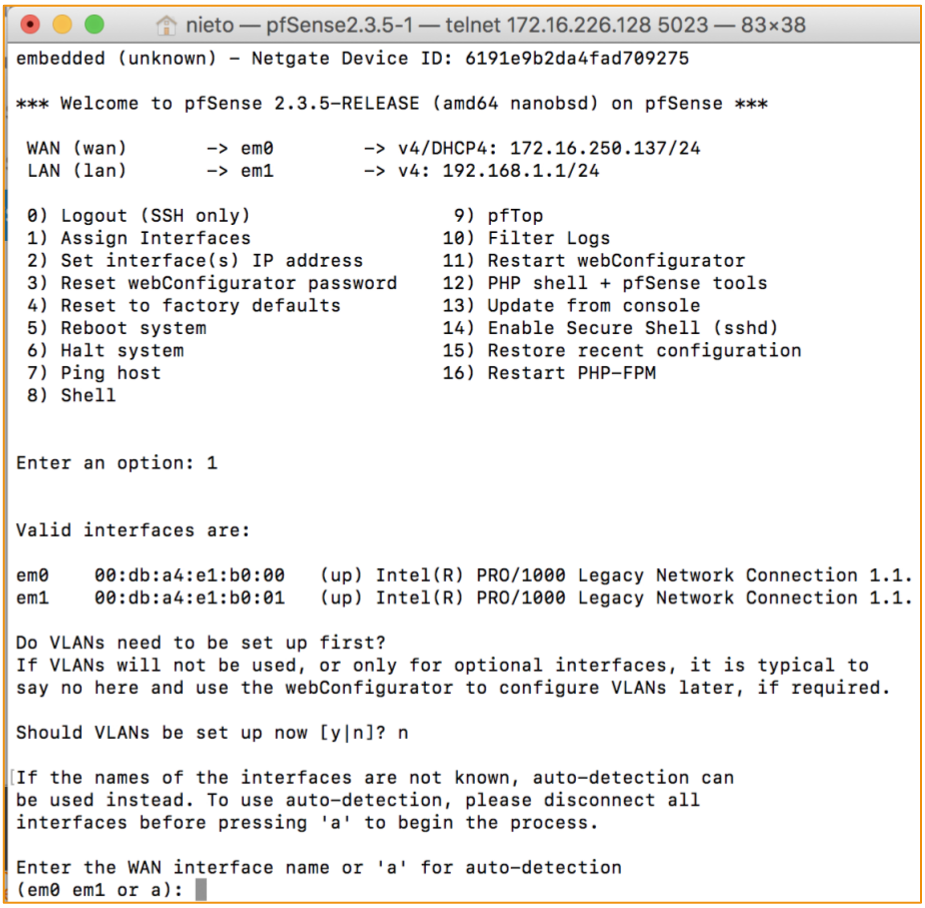


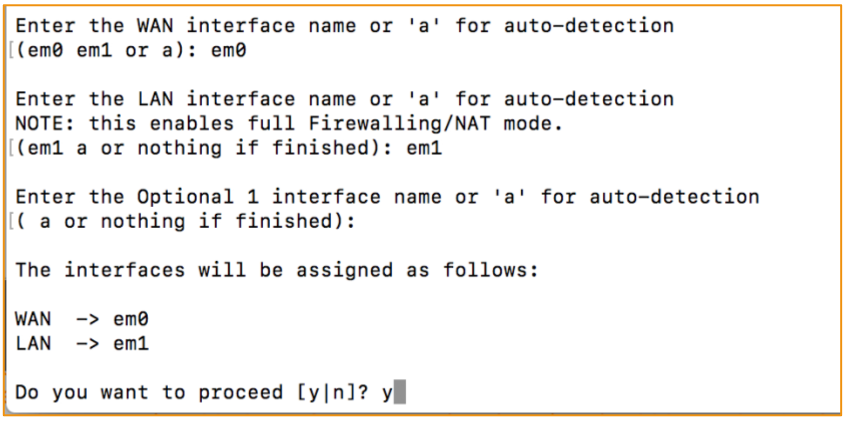
Figure 81. Including pfSense into a network

Thereafter, the student must configure the network interfaces using the console of the element pfSense. In particular, **em0 and em1** will be assigned for WAN and LAN respectively:



```
embedded (unknown) - Netgate Device ID: 6191e9b2da4fad709275

*** Welcome to pfSense 2.3.5-RELEASE (amd64 nanobsd) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 172.16.250.137/24
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24

 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: 1


Valid interfaces are:

em0    00:db:a4:e1:b0:00   (up) Intel(R) PRO/1000 Legacy Network Connection 1.1.
em1    00:db:a4:e1:b0:01   (up) Intel(R) PRO/1000 Legacy Network Connection 1.1.

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 or a):
```

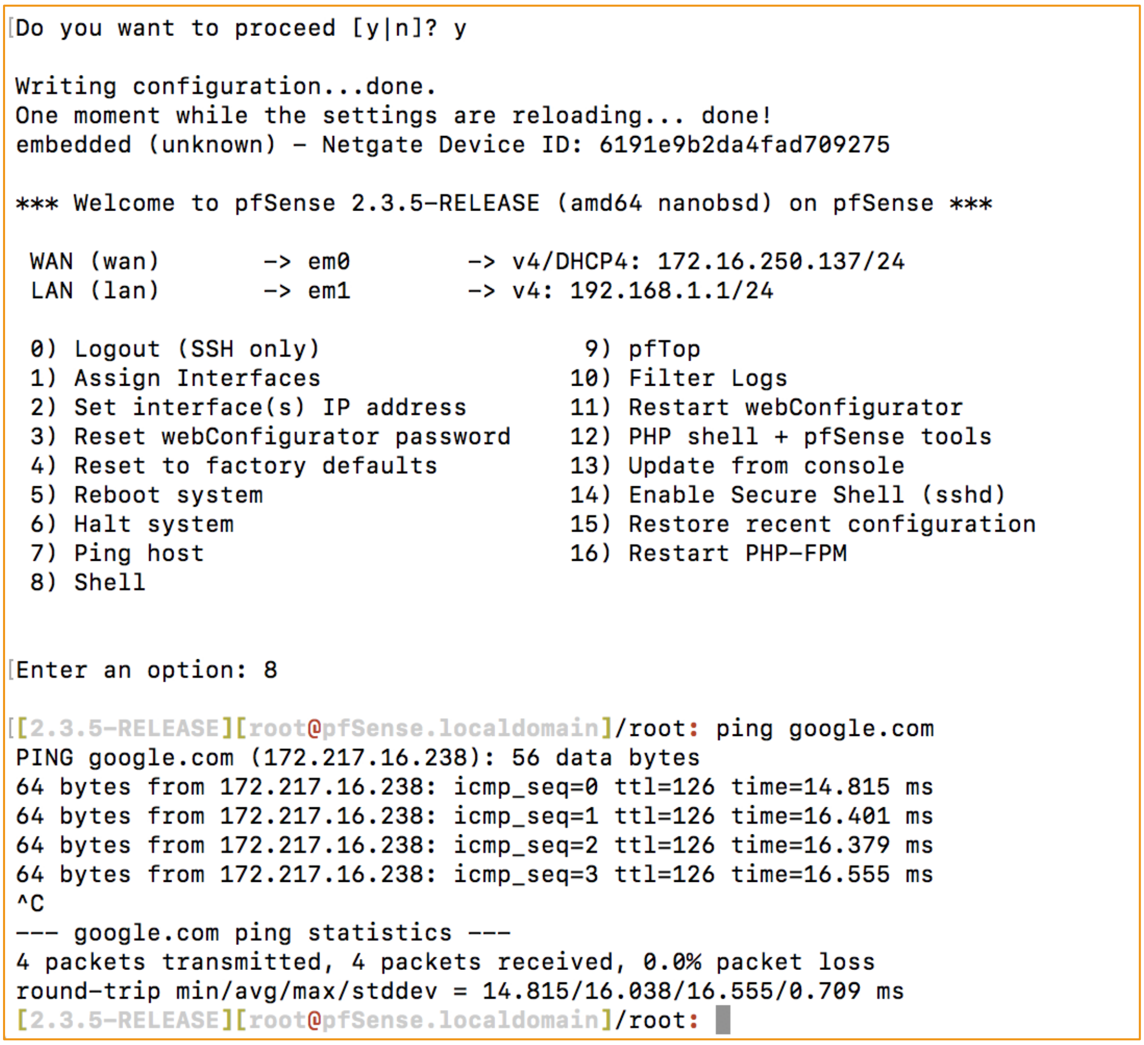
Figure 82. pfSense console



```
Enter the WAN interface name or 'a' for auto-detection
(em0 em1 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 a or nothing if finished): em1

Enter the Optional 1 interface name or 'a' for auto-detection
( a or nothing if finished):

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1

Do you want to proceed [y|n]? y
```

Figure 83. pfSense. Interface setup

The student must check the access to the Internet using the shell in pfSense as is shown in Figure 84. Note that, by default, pfSense configures the LAN in the network 192.168.1.1/24. Therefore, it is more than advisable to reserve this range of IP addresses for this network.

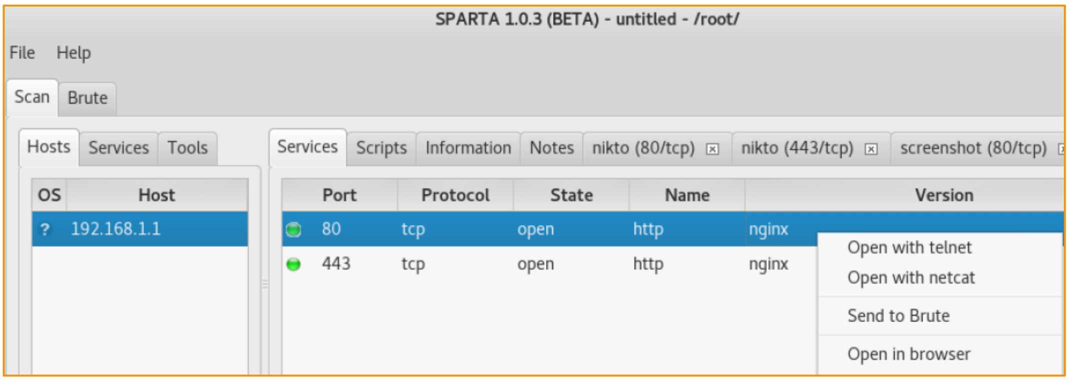


```
[Do you want to proceed [y|n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
embedded (unknown) - Netgate Device ID: 6191e9b2da4fad709275

*** Welcome to pfSense 2.3.5-RELEASE (amd64 nanobsd) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 172.16.250.137/24
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24

 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: 8

[[2.3.5-RELEASE][root@pfSense.localdomain]/root: ping google.com
PING google.com (172.217.16.238): 56 data bytes
64 bytes from 172.217.16.238: icmp_seq=0 ttl=126 time=14.815 ms
64 bytes from 172.217.16.238: icmp_seq=1 ttl=126 time=16.401 ms
64 bytes from 172.217.16.238: icmp_seq=2 ttl=126 time=16.379 ms
64 bytes from 172.217.16.238: icmp_seq=3 ttl=126 time=16.555 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 14.815/16.038/16.555/0.709 ms
[2.3.5-RELEASE][root@pfSense.localdomain]/root:
```

Figure 84. Access to the Internet

8.4 INSTALLING SNORT IN PFSENSE

In order to install Snort in pfSense, it is recommended to use the browser. The student may use the Kali to do that, for example, by analysing the open ports in the firewall and open the service in the browser (Figure 85).



OS	Host
?	192.168.1.1

Port	Protocol	State	Name	Version
80	tcp	open	http	nginx
443	tcp	open	http	nginx

Figure 85. Searching pfSense from Kali

The user/password to access with administrative privileges by default are: User: **admin**, Password: **pfsense**.

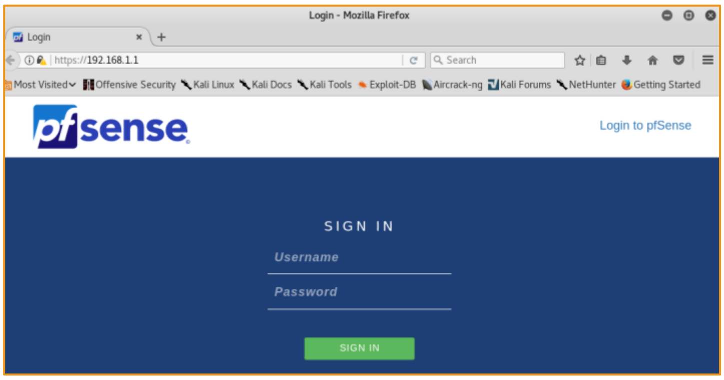
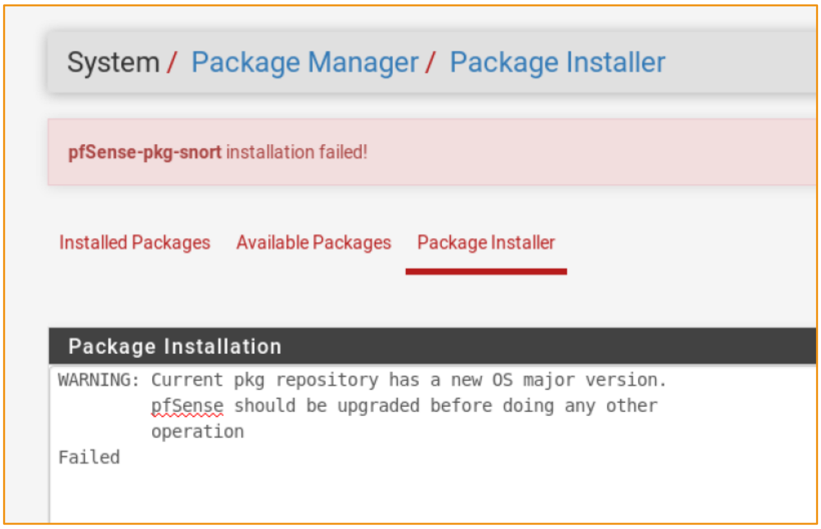


Figure 86. Accessing to pfSense from Kali

The packages available can be listed in System/Package Manager/Available Packages (Figure 90). However, before to install snort, the system must be updated in order to avoid the error shown in Figure 87.



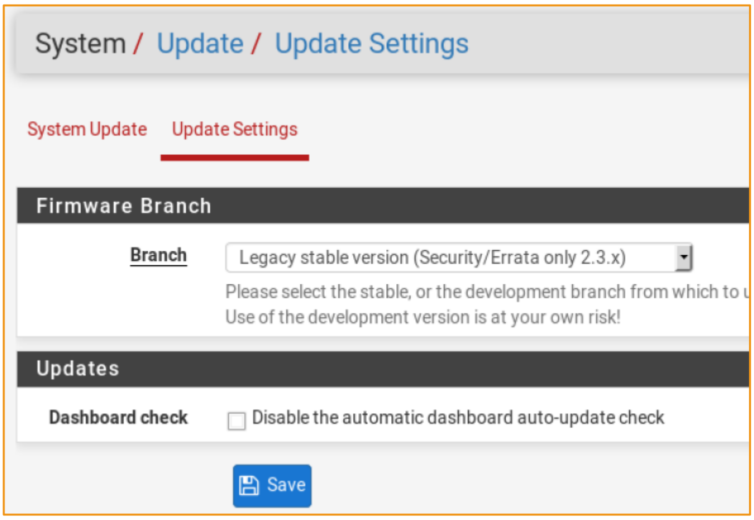
pfSense-pkg-snort installation failed!

```
WARNING: Current pkg repository has a new OS major version.
         pfSense should be upgraded before doing any other
         operation
Failed
```

Figure 87. Installing Snort in pfSense (fail)

8.4.1 UPDATE THE SYSTEM

The first step before the system update is to configure the update settings (Figure 88). The student must select "Legacy stable version (Security/Errata only 2.3.x)" to avoid errors during the updating.



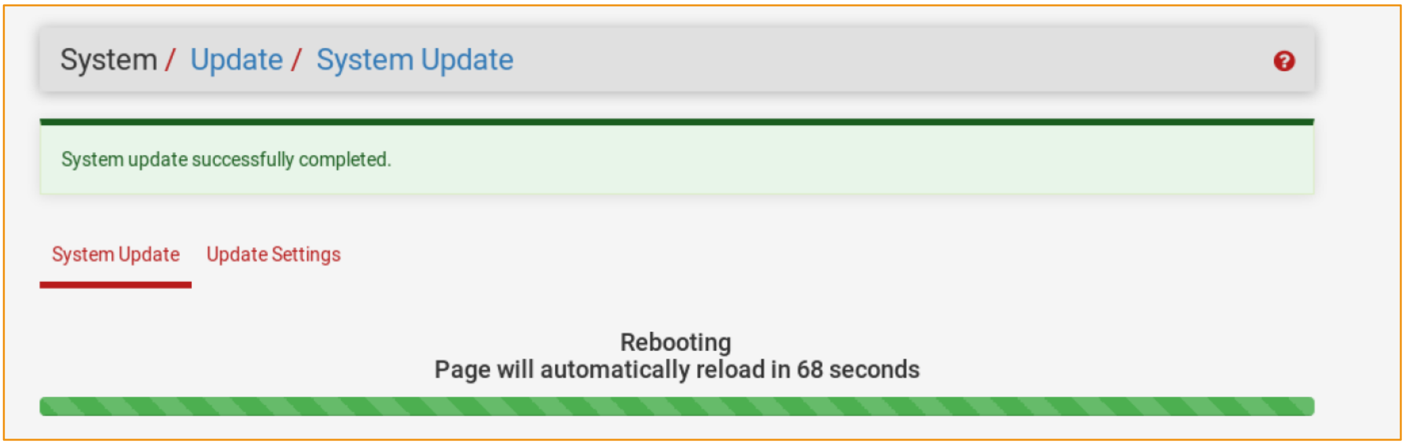
Branch: Legacy stable version (Security/Errata only 2.3.x)

Please select the stable, or the development branch from which to u
Use of the development version is at your own risk!

Dashboard check: □ Disable the automatic dashboard auto-update check

Figure 88. pfSense - Update Settings

After the previous step, the system can be updated in System/Update/System Update. Figure 90 shows the result after the software update in case everything went as expected.


System / Update / System Update

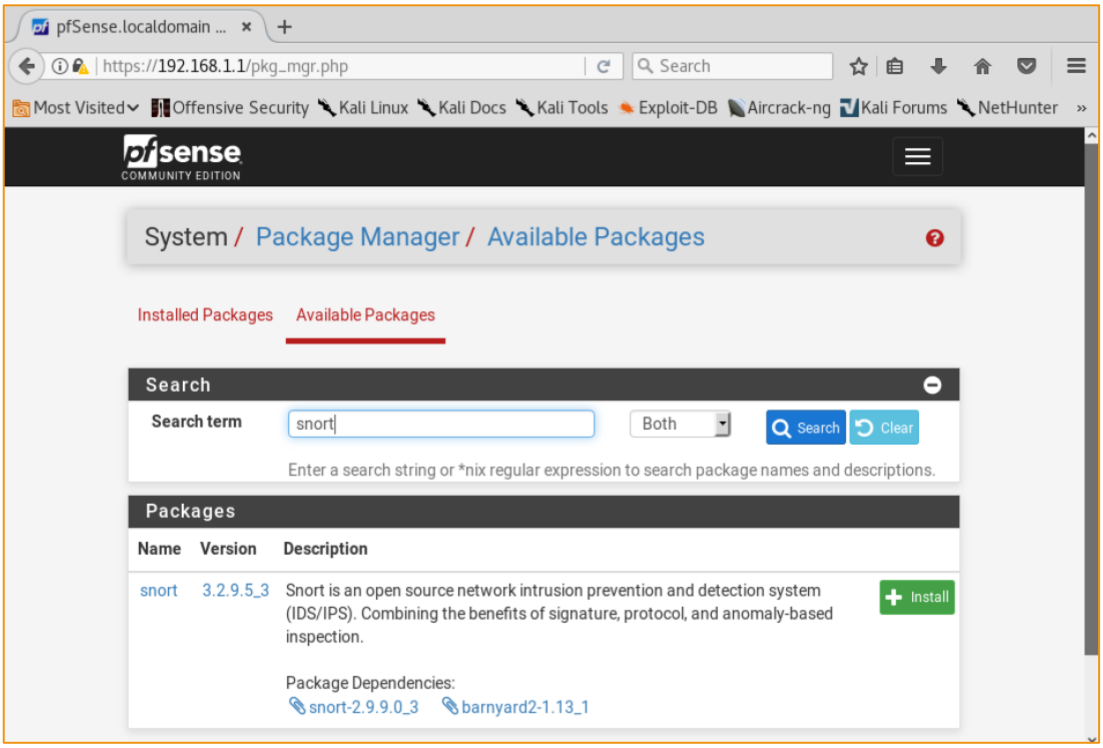
System update successfully completed.

Rebooting
Page will automatically reload in 68 seconds

Figure 89. pfSense - System Updated

8.4.2 SNORT IN PFSENSE

Once the system was updated, snort can be installed. To do that, the student may search the package for snort in System/Package Manager/Available Packages.



System / Package Manager / Available Packages

Search

Search term: snort | Both

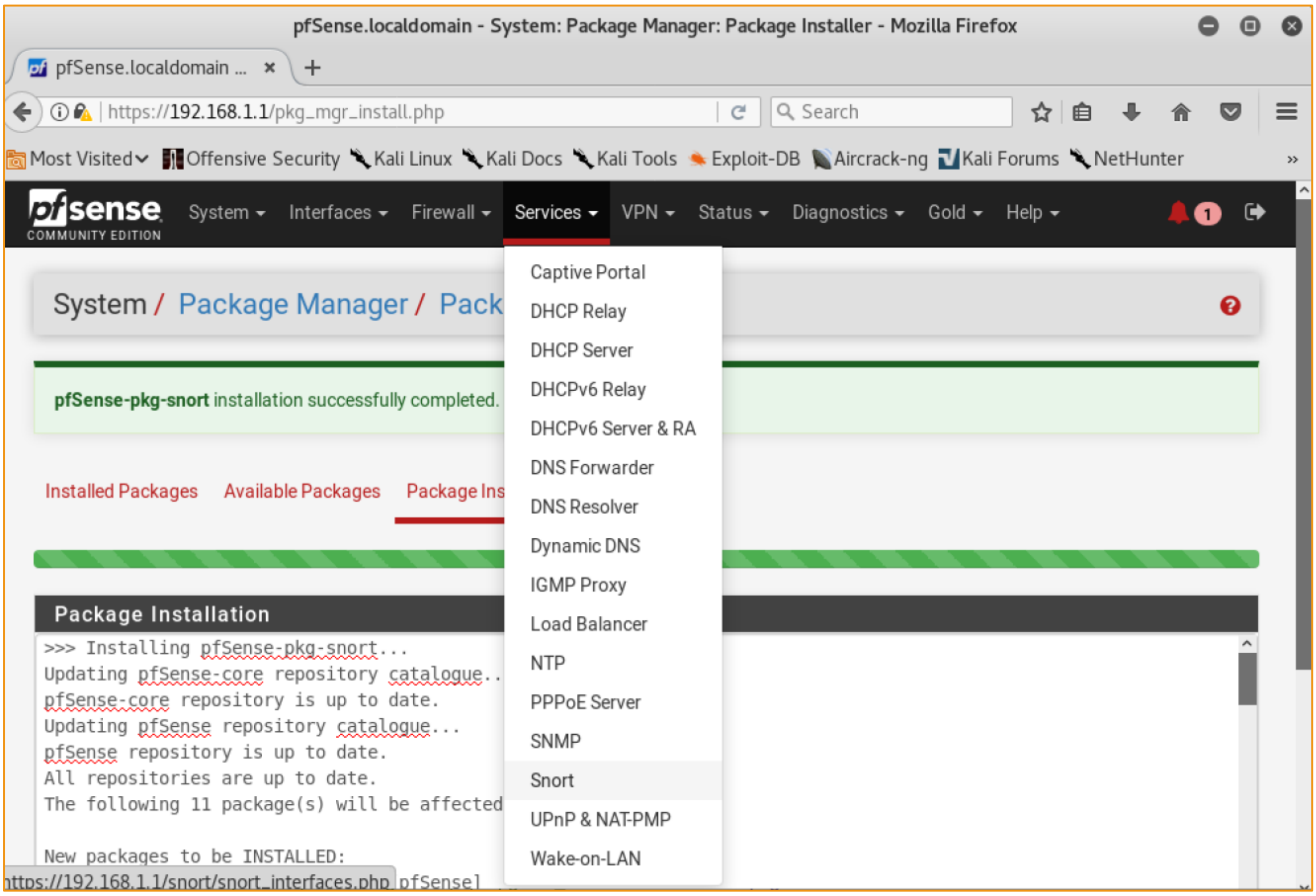
Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description
snort	3.2.9.5_3	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection. Package Dependencies: snort-2.9.9.0_3 barnyard2-1.13_1

Figure 90. pfSense packet manager - searching for Snort

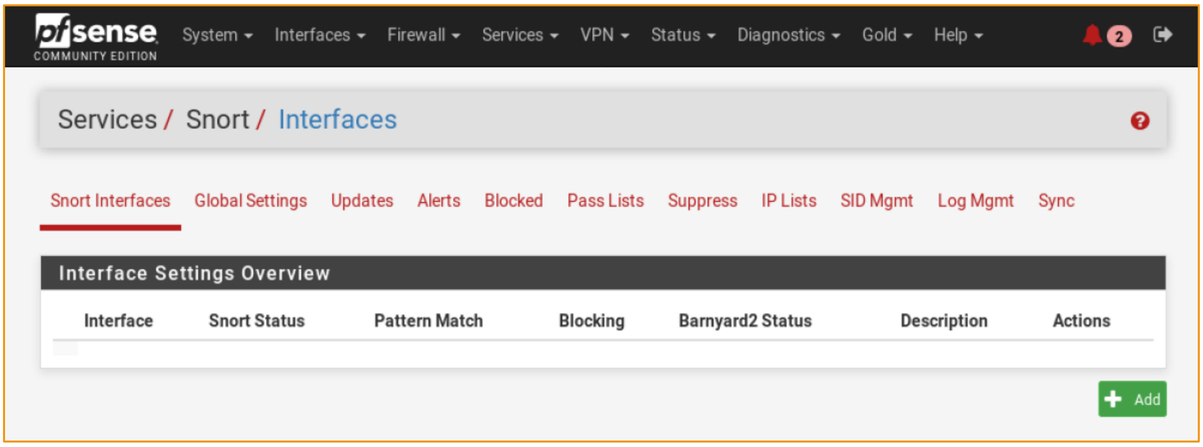
After the installation of the package, it can be configured through the tab “Services/Snort”, such as Figure 91 shows. There are several options that can be configured, as Figure 92 shows. It is critical to update the set of rules before to use snort (Figure 93).



pfSense-pkg-snort installation successfully completed.

```
>>> Installing pfSense-pkg-snort...
Updating pfSense-core repository catalogue..
pfSense-core repository is up to date.
Updating pfSense repository catalogue...
pfSense repository is up to date.
All repositories are up to date.
The following 11 package(s) will be affected

New packages to be INSTALLED:
pfSense]
```

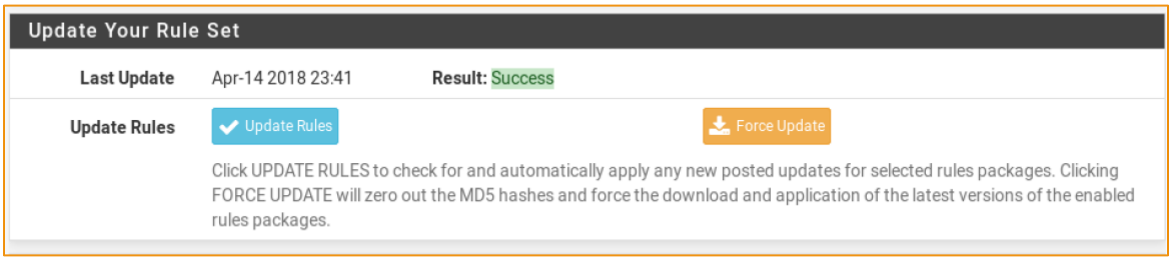
Figure 91. Snort installed in pfSense



Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking	Barnyard2 Status	Description	Actions

Figure 92. Snort options in pfSense



Update Your Rule Set

Last Update Apr-14 2018 23:41 **Result:** Success

Update Rules

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

Figure 93. Rule set updated - pfSense and Snort

8.5 PACKAGES INSTALLED IN THE GNS3 PROJECT "SNORTSG-IN-FIRE"

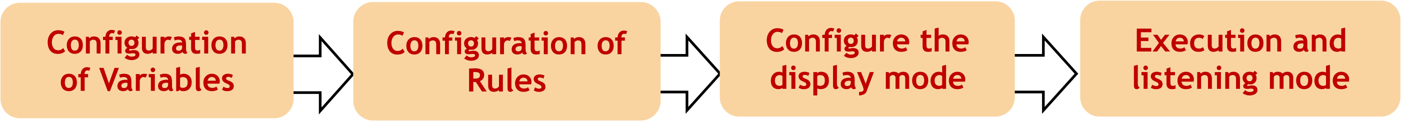
The following packages have been installed in the element pfSense in the project "SnortSG-in-FIRE.gns3project":

Package	Version	Description
Snort	3.2.9.6_1	Open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.
Suricata		High Performance Network IDS, IPS and Security Monitoring engine by OSIF.
Lightsquid	3.0.6_4	High performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package.
pfBlockerNG	2.1.2_3	Next generation of pfBlocker. Manage IPv4/v6 List Sources into 'Deny, Permit or Match' formats. GeoIP database by MaxMind Inc. (GeoLite2 Free version). De-duplication, suppression, and reputation enhancements. Provision to download from diverse list formats. Advanced integration for proofpoint ET IQRisk IP reputation Threat sources. Domain Name (DNSBL) blocking via Unbound DNS Resolver.
squid	0.4.43_1	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as HTTP/HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP.
squidGuard	1.16.4	High performance web proxy URL filter.

9 SNORT

Snort is a **signature-based IDS** that can work as HIDS (when installed in a host) or as NIDS (when installed in another location or filtering device (e.g. pfSense) in the network).

In any case, the ***power* of Snort** is on the **rules defined to trigger the alerts**. The following steps must be followed in order to configure Snort. Note that, if Snort has been installed in a network element (e.g. pfSense), then some steps may vary.


Configuration of Variables → Configuration of Rules → Configure the display mode → Execution and listening mode

Snort can be configured editing the file **/etc/snort/snort.conf**. In such a file, a basic sample snort configuration can be found. As the student can observe, there are **multiple steps defined in the file**. However, the basic configuration in order to make some tests can be done in four steps.

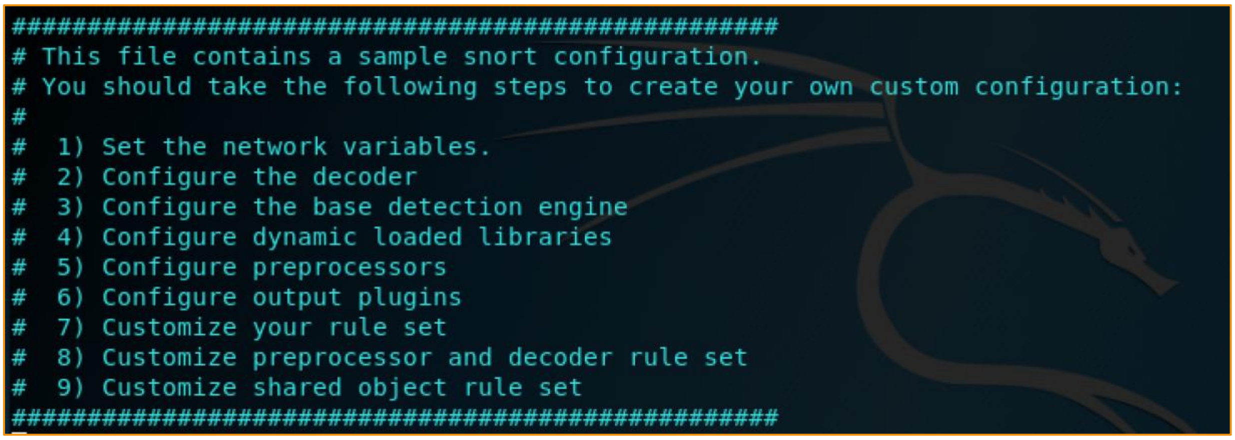

```
###################################################
# This file contains a sample snort configuration.
# You should take the following steps to create your own custom configuration:
#
#  1) Set the network variables.
#  2) Configure the decoder
#  3) Configure the base detection engine
#  4) Configure dynamic loaded libraries
#  5) Configure preprocessors
#  6) Configure output plugins
#  7) Customize your rule set
#  8) Customize preprocessor and decoder rule set
#  9) Customize shared object rule set
###################################################
```

Figure 94. /etc/snort/snort.conf

Of course, the student can define his own configuration file to be used by Snort. However, it is recommended to make some initial tests using the file /etc/snort/snort.conf.

9.1 STEP1. CONFIGURATION OF NETWORK VARIABLES

The first step is to configure Snort in order to set up basic parameters, such as the network from which it will receive the packets. As a first example, HOME_NET is for the local interface (host in which Snort is running; HIDS).

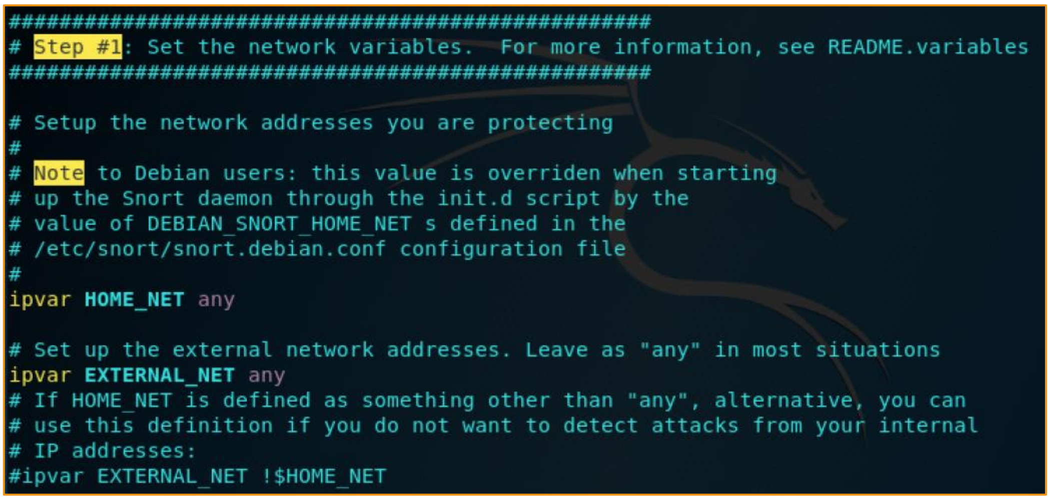
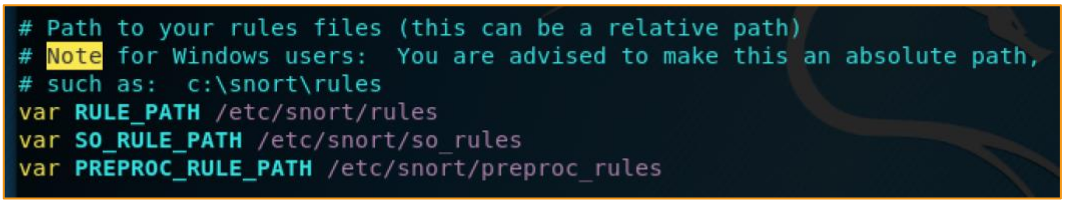

```
###################################################
# Step #1: Set the network variables.  For more information, see README.variables
###################################################

# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET any

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET
```

Figure 95. Network variables I

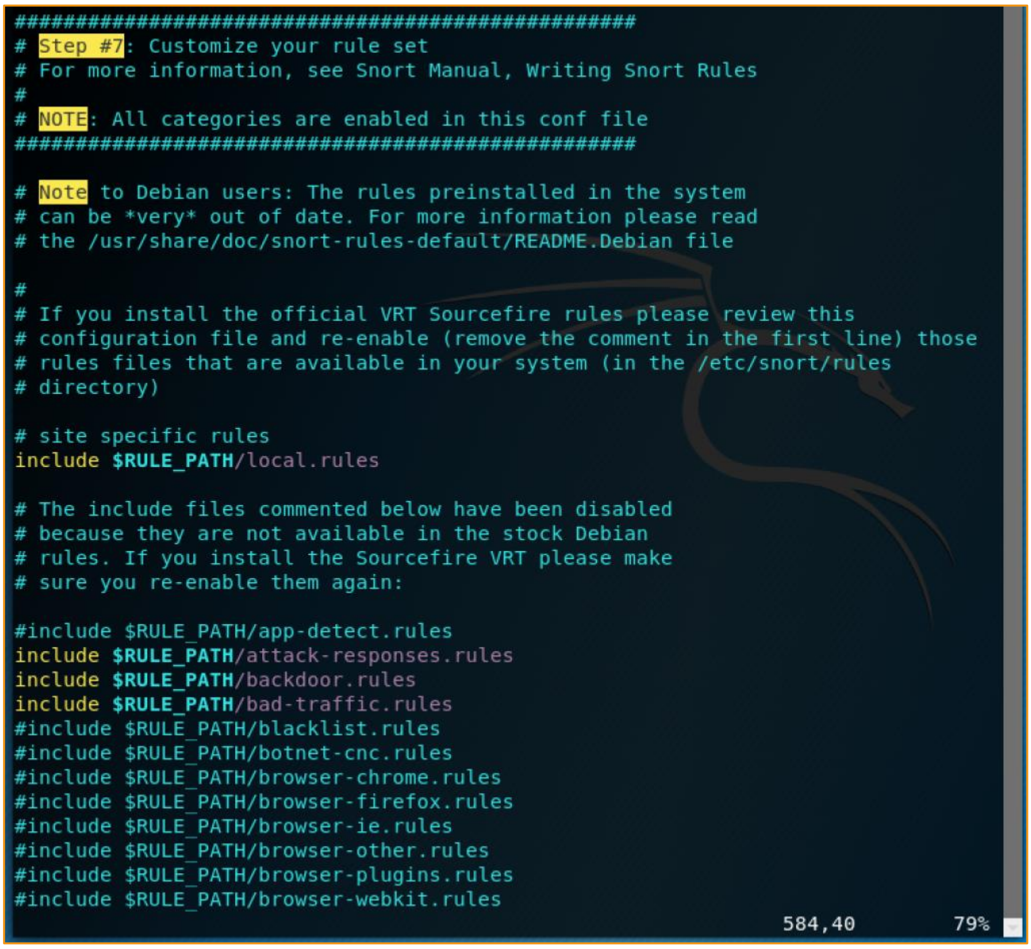


```
# Path to your rules files (this can be a relative path)
# Note for Windows users:  You are advised to make this an absolute path,
# such as:  c:\snort\rules
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules
```

Figure 96. Network variables II

9.2 STEP2. CONFIGURATION OF RULES

The objective is to configure the type of indicators that will raise an alert. In other words, the objective is to describe the attacks that will be detected. The rules can be found in separate files that are listed in the configuration file. The default path for rules is in RULE_PATH, which is **/etc/snort/rules**, according with the definition of the variable.

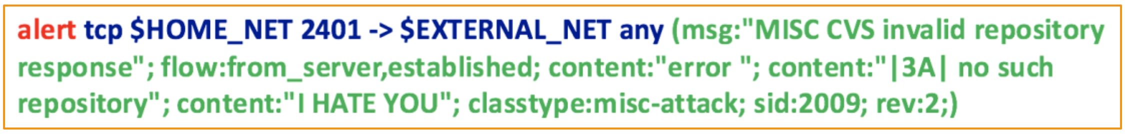


```
###################################################
# Step #7: Customize your rule set
# For more information, see Snort Manual, Writing Snort Rules
#
# NOTE: All categories are enabled in this conf file
###################################################

# Note to Debian users: The rules preinstalled in the system
# can be *very* out of date. For more information please read
# the /usr/share/doc/snort-rules-default/README.Debian file

#
# If you install the official VRT Sourcefire rules please review this
# configuration file and re-enable (remove the comment in the first line) those
# rules files that are available in your system (in the /etc/snort/rules
# directory)

# site specific rules
include $RULE_PATH/local.rules

# The include files commented below have been disabled
# because they are not available in the stock Debian
# rules. If you install the Sourcefire VRT please make
# sure you re-enable them again:

#include $RULE_PATH/app-detect.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/bad-traffic.rules
#include $RULE_PATH/blacklist.rules
#include $RULE_PATH/botnet-cnc.rules
#include $RULE_PATH/browser-chrome.rules
#include $RULE_PATH/browser-firefox.rules
#include $RULE_PATH/browser-ie.rules
#include $RULE_PATH/browser-other.rules
#include $RULE_PATH/browser-plugins.rules
#include $RULE_PATH/browser-webkit.rules
                                                         584,40        79%
```

Figure 97. Rule set in Snort

The student can comment these rules and include new ones, or simply add new ones. But **it is very, very important to comment the rules that will be not used and check that there are not duplicate IDs.**

The format of the rules in snort is quite similar to the description provided for Suricata rules (in the magisterial lessons):

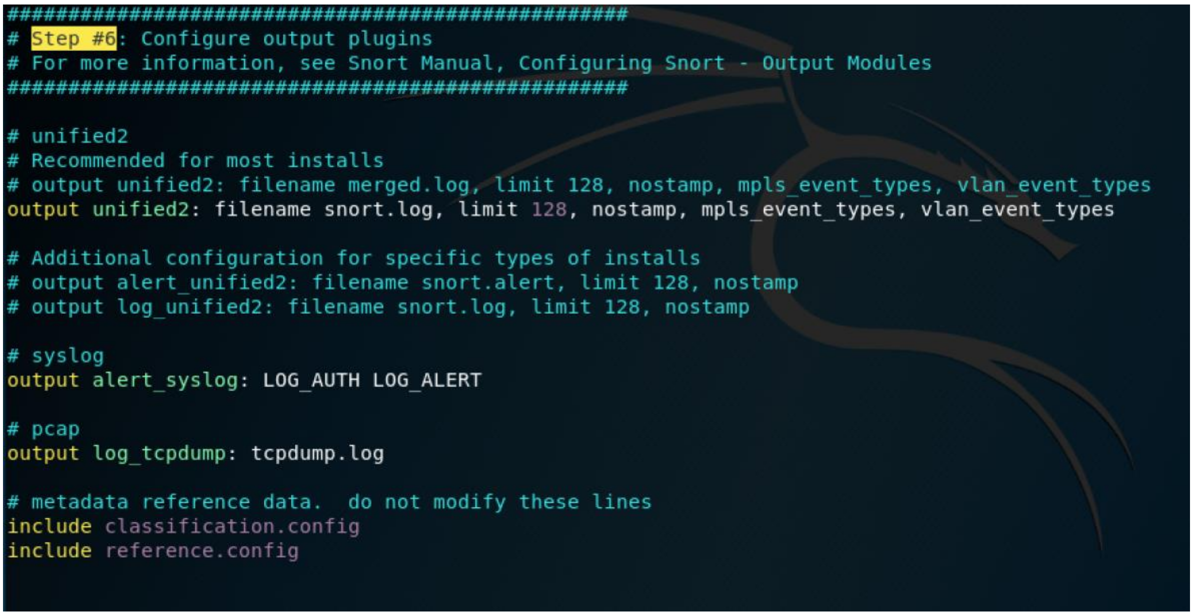


```
alert tcp $HOME_NET 2401 -> $EXTERNAL_NET any (msg:"MISC CVS invalid repository response"; flow:from_server,established; content:"error "; content:"|3A| no such repository"; content:"I HATE YOU"; classtype:misc-attack; sid:2009; rev:2;)
```

Figure 98. Structure of a rule in Snort and Suricata - Action (red), header (blue), rule options (green)

9.3 STEP3. CONFIGURE THE DISPLAY MODE

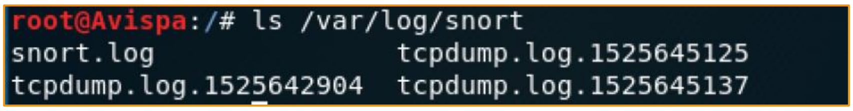
In this step it will be decided how the evidence will be displayed. The options for "output" are listed in snort.conf. **Note that the option for unified2 has been commented and the options for pcap and syslog have been uncommented.**



```
###################################################
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output Modules
###################################################

# unified2
# Recommended for most installs
# output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, vlan_event_types
output unified2: filename snort.log, limit 128, nostamp, mpls_event_types, vlan_event_types

# Additional configuration for specific types of installs
# output alert_unified2: filename snort.alert, limit 128, nostamp
# output log_unified2: filename snort.log, limit 128, nostamp

# syslog
output alert_syslog: LOG_AUTH LOG_ALERT

# pcap
output log_tcpdump: tcpdump.log

# metadata reference data.  do not modify these lines
include classification.config
include reference.config
```

Figure 99. Configure output Snort

Moreover, the option (-l) stores the logs in a specific directory. By default, the logs are stored in **/var/log/snort**.



```
root@Avispa:/# ls /var/log/snort
snort.log                tcpdump.log.1525645125
tcpdump.log.1525642904   tcpdump.log.1525645137
```

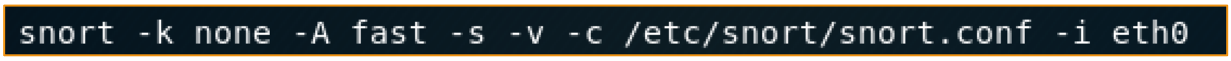
Figure 100. Default location of logs for Snort

9.4 STEP4. EXECUTION AND LISTENING MODE

If the configuration file has been modified, the **service snort must be stopped and started again.** To do that:

```
service snort stop
service snort start
```

In the following example snort is executed using the rules defined in the file **/etc/snort/snort.conf**.



```
snort -k none -A fast -s -v -c /etc/snort/snort.conf -i eth0
```

Figure 101. Execution of Snort using the rules in /etc/snort/snort.conf

However, note that the option for verbose (-v) shows all what is received by the network interface, and is time and resource consuming. **REMEMBER, use the option "-l" (without quotes) to store the logs. "-A fast" must be used to save the alert in a file (in /var/log/snort). "-A console" is used to print the alert as log in the console (terminal).**

9.5 COUNTERMEASURES

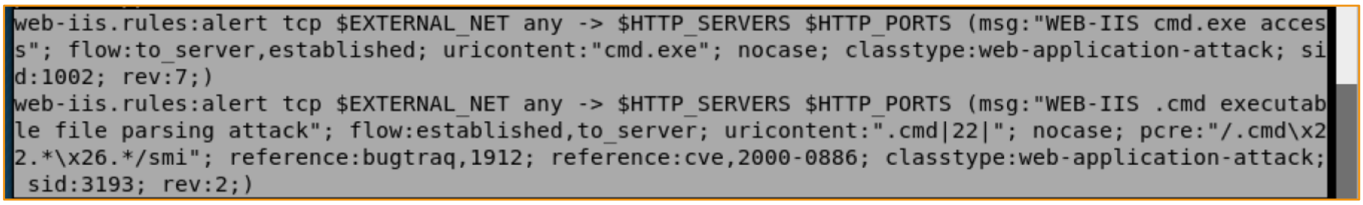
The actions "drop" and "reject" instead of "alert" can be used to "drop" or "reject" the packet which satisfies the conditions.

9.6 PRACTICAL EXAMPLE

In order to check if Snort is properly configured, the student can make the following test:

1. Once configured, execute snort with the command “snort -v -c /etc/snort/snort.conf”.
2. In another window (terminal), execute a command with the following **structure,** where $EXTERNAL_HOST is a host that you have permission to access for this exercise: “wget http://$EXTERNAL_HOST/cmd.exe”. This should raise an alert. For example, the student can try:
   `wget www.nics.uma.es/winnt/system32/cmd.exe`
3. Check the .log file (in **/etc/snort/logs** according to our configuration).

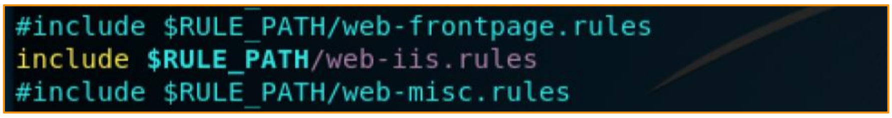
These are the rules that are being applied (note that in the rules the state “established” is indicated):



```
web-iis.rules:alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-IIS cmd.exe acces
s"; flow:to_server,established; uricontent:"cmd.exe"; nocase; classtype:web-application-attack; si
d:1002; rev:7;)
web-iis.rules:alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-IIS .cmd executab
le file parsing attack"; flow:established,to_server; uricontent:".cmd|22|"; nocase; pcre:"/.cmd\x2
2.*\x26.*/smi"; reference:bugtraq,1912; reference:cve,2000-0886; classtype:web-application-attack;
 sid:3193; rev:2;)
```

Figure 102. Rules in web-iis.rules related to the practical example

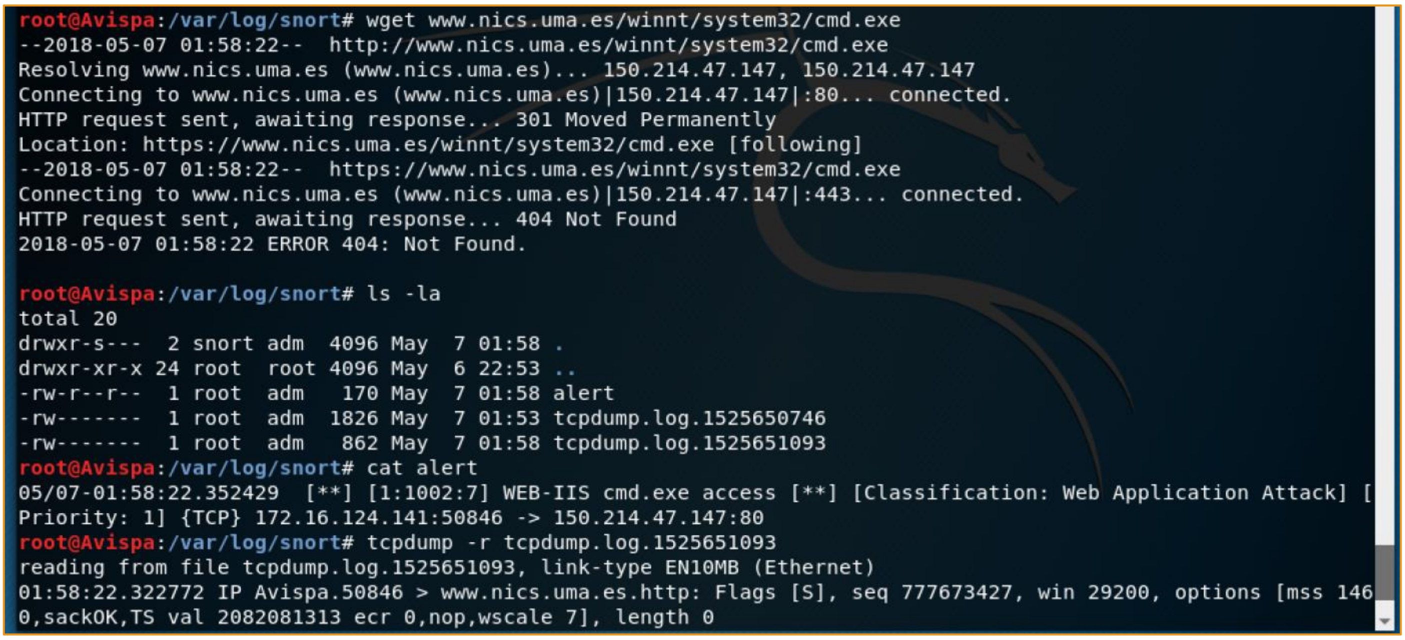
Of course, the file with the rules must be enabled in snort.conf in order to use the rules.



```
#include $RULE_PATH/web-frontpage.rules
include $RULE_PATH/web-iis.rules
#include $RULE_PATH/web-misc.rules
```

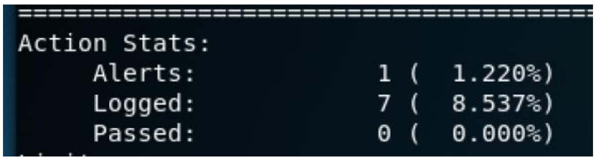
Figure 103. Rules for the exercise enabled in Snort

The following figures shows some results after the practical exercise.



```
root@Avispa:/var/log/snort# wget www.nics.uma.es/winnt/system32/cmd.exe
--2018-05-07 01:58:22--  http://www.nics.uma.es/winnt/system32/cmd.exe
Resolving www.nics.uma.es (www.nics.uma.es)... 150.214.47.147, 150.214.47.147
Connecting to www.nics.uma.es (www.nics.uma.es)|150.214.47.147|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.nics.uma.es/winnt/system32/cmd.exe [following]
--2018-05-07 01:58:22--  https://www.nics.uma.es/winnt/system32/cmd.exe
Connecting to www.nics.uma.es (www.nics.uma.es)|150.214.47.147|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
2018-05-07 01:58:22 ERROR 404: Not Found.

root@Avispa:/var/log/snort# ls -la
total 20
drwxr-s---  2 snort adm  4096 May  7 01:58 .
drwxr-xr-x 24 root  root 4096 May  6 22:53 ..
-rw-r--r--  1 root  adm   170 May  7 01:58 alert
-rw-------  1 root  adm  1826 May  7 01:53 tcpdump.log.1525650746
-rw-------  1 root  adm   862 May  7 01:58 tcpdump.log.1525651093
root@Avispa:/var/log/snort# cat alert
05/07-01:58:22.352429  [**] [1:1002:7] WEB-IIS cmd.exe access [**] [Classification: Web Application Attack] [
Priority: 1] {TCP} 172.16.124.141:50846 -> 150.214.47.147:80
root@Avispa:/var/log/snort# tcpdump -r tcpdump.log.1525651093
reading from file tcpdump.log.1525651093, link-type EN10MB (Ethernet)
01:58:22.322772 IP Avispa.50846 > www.nics.uma.es.http: Flags [S], seq 777673427, win 29200, options [mss 146
0,sackOK,TS val 2082081313 ecr 0,nop,wscale 7], length 0
```

Figure 104. wget and alert generated by Snort



```
=======================================
Action Stats:
     Alerts:            1 (  1.220%)
     Logged:            7 (  8.537%)
     Passed:            0 (  0.000%)
```

Figure 105. Summary of alerts and logs after the execution of Snort

9.7 USEFUL COMMANDS AND UTILITIES

Next table shows a set of commands that can be useful to process and interpret .pcap files.

Command	Objective
snort -c /etc/snort/snort.conf -r file.pcap -A full	Shows the vulnerability that was attacked (if the rule was configured in Snort).
tshark -r file.pcap -q -z ip_hosts,tree	Shows the IP which are involved.
p0f -r file.pcap "ip host 10.10.10.10"	Shows information about the computer. Use "p0f --help" to more information ("p" zero "f").
tshark -r file.pcap -q -z conv,tcp -nn	Number of sessions TCP.
tshark -r file.pcap -t r | tail -n 1	Duration.
tcpdump -r file.pcap icmp | head	Show the header of the ICMP packets (e.g. to deduce the IP address of the attacker).

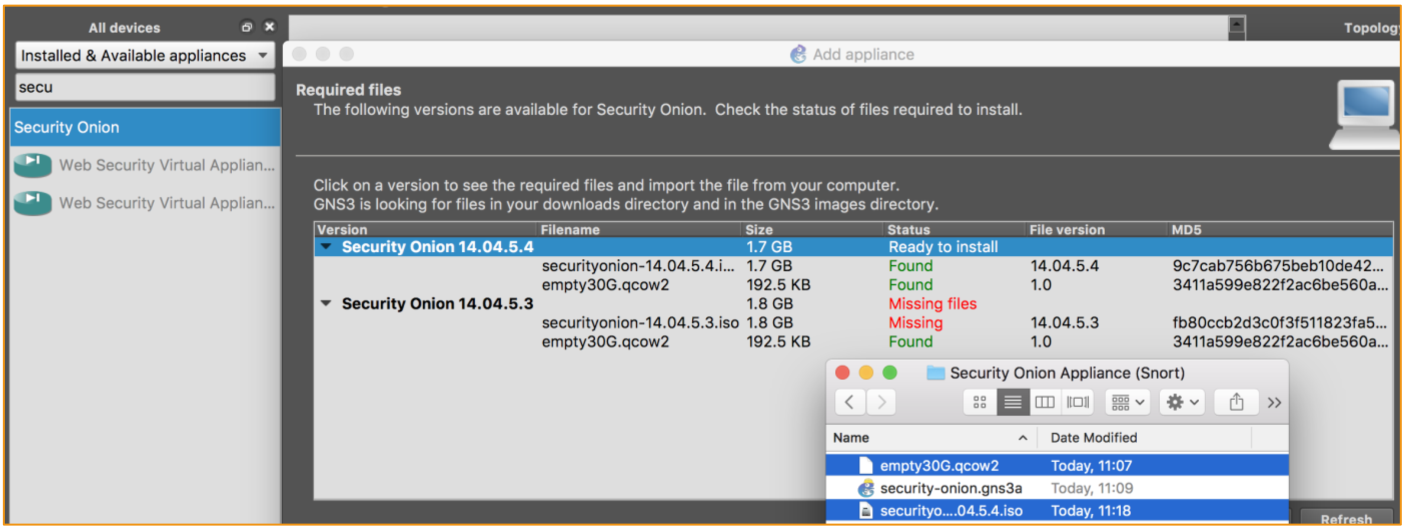
In addition, using "follow TCP stream" in Wireshark it is possible to extract the files updated to the victim.

Moreover, once that snort is running, if the student connects to "http://www.testmyids.com/" it is possible to check if the IDS is generating alerts properly.

10 SECURITY ONION (INTRUSION DETECTION)

"Security Onion is a Linux distro for intrusion detection, network security monitoring, and log management. It's based on Ubuntu and contains Snort, Suricata, Bro, OSSEC, Sguil, Squert, ELSA, Xplico, NetworkMiner, and many other security tools.". More information about this appliance can be found in GitHub: https://github.com/Security-Onion-Solutions/security-onion/wiki/IntroductionToSecurityOnion.

The student can download this appliance for GNS3 from https://www.gns3.com/marketplace/appliance/security-onion, and the files for one of the supported versions from https://docs.gns3.com/appliances/security-onion.html#header. Furthermore, all the files are available for download in the virtual campus, from:


All devices
Installed & Available appliances
secu
Security Onion
Web Security Virtual Applian...
Web Security Virtual Applian...
Topolog
Add appliance
Refresh

Required files

The following versions are available for Security Onion. Check the status of files required to install.

Click on a version to see the required files and import the file from your computer.
GNS3 is looking for files in your downloads directory and in the GNS3 images directory.

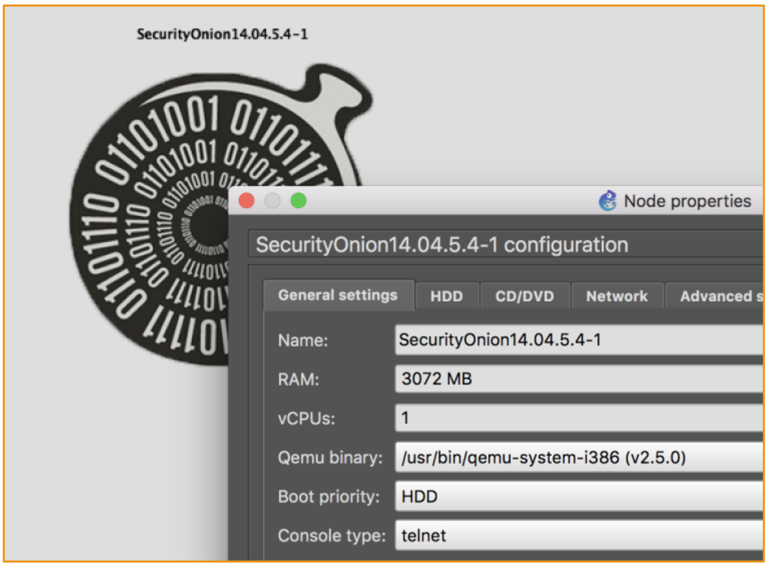
Version	Filename	Size	Status	File version	MD5
Security Onion 14.04.5.4		1.7 GB	Ready to install		
	securityonion-14.04.5.4.i...	1.7 GB	Found	14.04.5.4	9c7cab756b675beb10de42...
	empty30G.qcow2	192.5 KB	Found	1.0	3411a599e822f2ac6be560a...
Security Onion 14.04.5.3		1.8 GB	Missing files		
	securityonion-14.04.5.3.iso	1.8 GB	Missing	14.04.5.3	fb80ccb2d3c0f3f511823fa5...
	empty30G.qcow2	192.5 KB	Found	1.0	3411a599e822f2ac6be560a...

Security Onion Appliance (Snort)

Name	Date Modified
empty30G.qcow2	Today, 11:07
security-onion.gns3a	Today, 11:09
securityo....04.5.4.iso	Today, 11:18

Figure 106. Security Onion in GNS3

This appliance requires 3072MB of RAM in order to run. User: **squil**, Password: **squert**.



SecurityOnion14.04.5.4-1 configuration

Name: SecurityOnion14.04.5.4-1
RAM: 3072 MB
vCPUs: 1
Qemu binary: /usr/bin/qemu-system-i386 (v2.5.0)
Boot priority: HDD
Console type: telnet

Figure 107. Security Onion in GNS3

11 ALPINE LINUX

Alpine is a lightweight Linux system available as GNS3 appliance.

11.1 CONFIGURE THE NETWORK INTERFACE

It is necessary to configure the network interface in order to connect this little linux system with the Internet you can do it by editing the configuration file **/etc/network/interfaces**. However, it is recommended to make the changes using GNS3 before starting the node. The DNS can be edited in **/etc/resolv.conf** file. Each **"nameserver"** line defines a DNS server, that are prioritized in the order the system finds them in the file. **"nameserver 8.8.8.8" (without the quotation) must be included.**

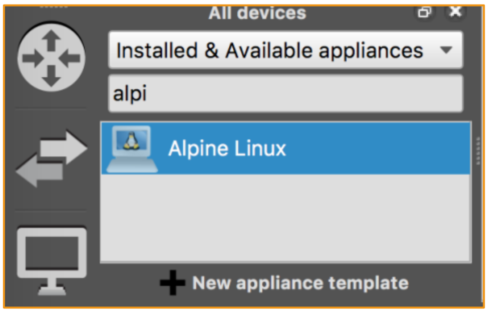
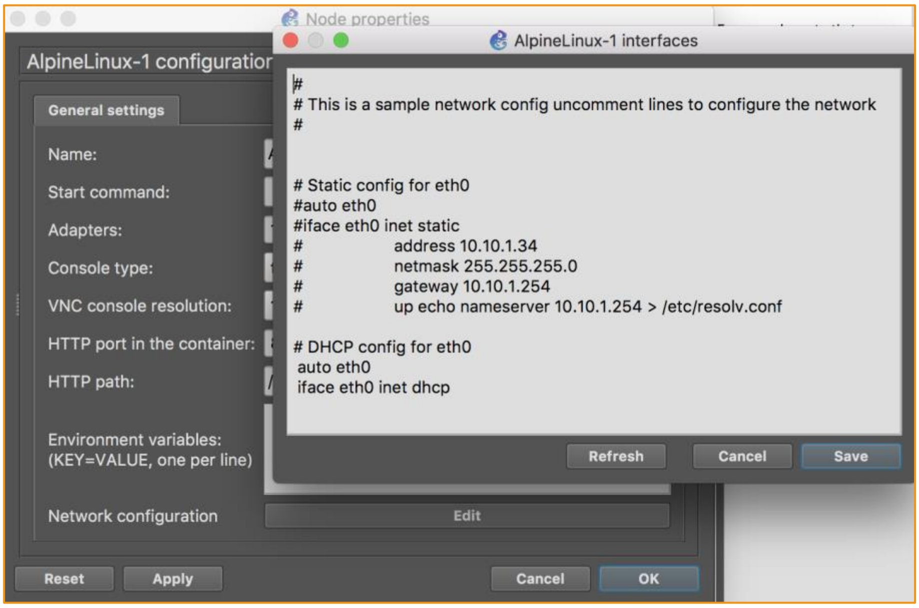


Figure 108. Alpine Linux in GNS3



```
#
# This is a sample network config uncomment lines to configure the network
#


# Static config for eth0
#auto eth0
#iface eth0 inet static
#           address 10.10.1.34
#           netmask 255.255.255.0
#           gateway 10.10.1.254
#           up echo nameserver 10.10.1.254 > /etc/resolv.conf

# DHCP config for eth0
 auto eth0
 iface eth0 inet dhcp
```

Figure 109. Alpine Linux - configuring network interface

11.2 UPDATE AND UPGRADE

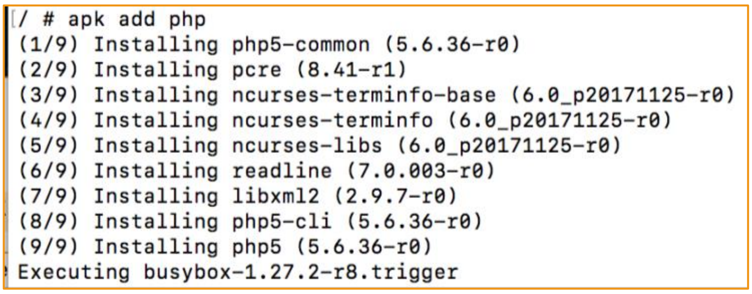
Next, check your connection to the Internet and update (apk update) and upgrade (apk upgrade) Alpine. More information about alpine: https://wiki.alpinelinux.org/wiki/Alpine_Linux_package_management

11.3 INSTALLING SNORT

Before to install snort, some dependencies must be installed in alpine. Here the student can find a complete guide about the installation of Snort in Alpine: https://wiki.alpinelinux.org/wiki/Intrusion_Detection_using_Snort. However, some changes must be addressed in order to fulfil the installation in our version of Alpine.

Go to the second step (16.3.2) to install Snort in Alpine to work with GNS3.

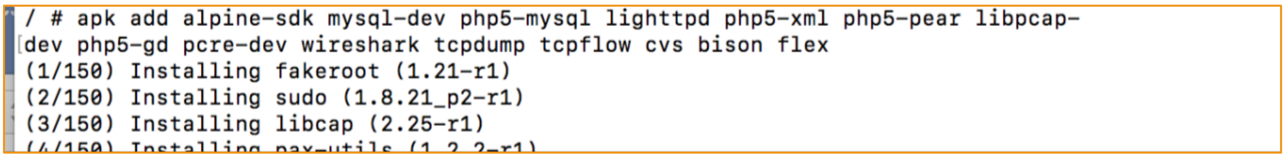
11.3.1 CHANGES IN THE DEPENDENT PACKAGES



```
/ # apk add php
(1/9) Installing php5-common (5.6.36-r0)
(2/9) Installing pcre (8.41-r1)
(3/9) Installing ncurses-terminfo-base (6.0_p20171125-r0)
(4/9) Installing ncurses-terminfo (6.0_p20171125-r0)
(5/9) Installing ncurses-libs (6.0_p20171125-r0)
(6/9) Installing readline (7.0.003-r0)
(7/9) Installing libxml2 (2.9.7-r0)
(8/9) Installing php5-cli (5.6.36-r0)
(9/9) Installing php5 (5.6.36-r0)
Executing busybox-1.27.2-r8.trigger
```

Figure 110. Installing php in Alpine

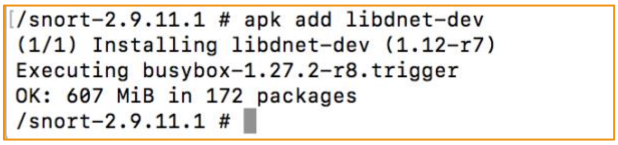
Install the pre-packaged components indicated in the previous link, but using “php5” instead of “php”.



```
/ # apk add alpine-sdk mysql-dev php5-mysql lighttpd php5-xml php5-pear libpcap-
dev php5-gd pcre-dev wireshark tcpdump tcpflow cvs bison flex
(1/150) Installing fakeroot (1.21-r1)
(2/150) Installing sudo (1.8.21_p2-r1)
(3/150) Installing libcap (2.25-r1)
(4/150) Installing pax-utils (1.2.2-r1)
```

Figure 111. Installing dependencies in Alpine

Install libdnet-dev.



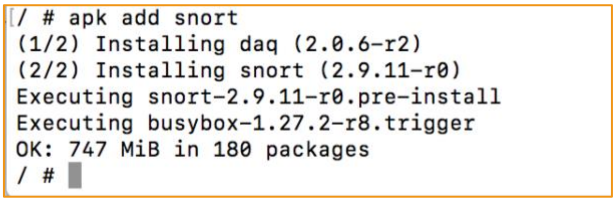
```
/snort-2.9.11.1 # apk add libdnet-dev
(1/1) Installing libdnet-dev (1.12-r7)
Executing busybox-1.27.2-r8.trigger
OK: 607 MiB in 172 packages
/snort-2.9.11.1 #
```

Figure 112. Installing libdnet

In addition, the installation guide includes additional steps (e.g. use mysql) that will be omitted here.

11.3.2 INSTALL SNORT (WITHOUT A FURTHER INSTALLATION)

Install snort:



```
/ # apk add snort
(1/2) Installing daq (2.0.6-r2)
(2/2) Installing snort (2.9.11-r0)
Executing snort-2.9.11-r0.pre-install
Executing busybox-1.27.2-r8.trigger
OK: 747 MiB in 180 packages
/ #
```

Figure 113. Install snort in Alpine

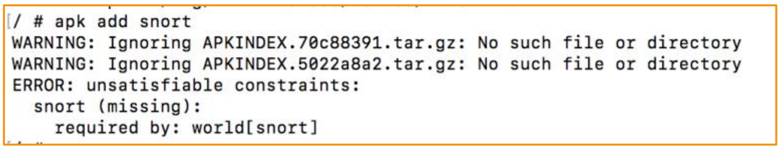
After this step, the student must consider the steps in “solving errors”.

11.4 TESTING

The student can use the Kali Linux in order to test the capability of Snort to detect attacks against the Alpine Linux. This will depend on the purpose of the HIDS; that is, the rules that will be configured to detect the attacks in Snort.

11.5 SOLVING ERRORS

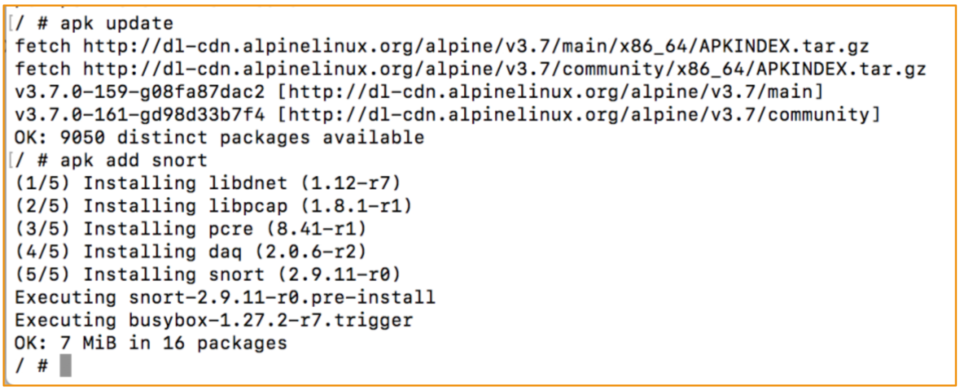
The following warnings and error are shown if “apk update” is not made **before to install the packages**.



```
/ # apk add snort
WARNING: Ignoring APKINDEX.70c88391.tar.gz: No such file or directory
WARNING: Ignoring APKINDEX.5022a8a2.tar.gz: No such file or directory
ERROR: unsatisfiable constraints:
  snort (missing):
    required by: world[snort]
```

Figure 114. WARNING: Ignoring APKINDEX

The error is easily solved by calling to “apk update” before the installation process.



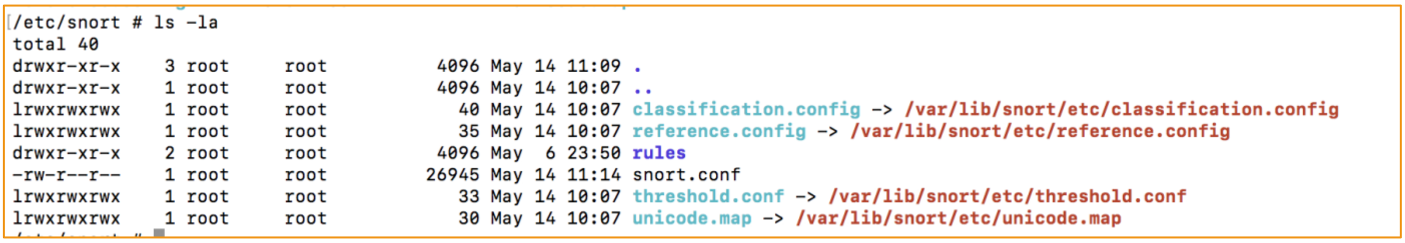
```
/ # apk update
fetch http://dl-cdn.alpinelinux.org/alpine/v3.7/main/x86_64/APKINDEX.tar.gz
fetch http://dl-cdn.alpinelinux.org/alpine/v3.7/community/x86_64/APKINDEX.tar.gz
v3.7.0-159-g08fa87dac2 [http://dl-cdn.alpinelinux.org/alpine/v3.7/main]
v3.7.0-161-gd98d33b7f4 [http://dl-cdn.alpinelinux.org/alpine/v3.7/community]
OK: 9050 distinct packages available
/ # apk add snort
(1/5) Installing libdnet (1.12-r7)
(2/5) Installing libpcap (1.8.1-r1)
(3/5) Installing pcre (8.41-r1)
(4/5) Installing daq (2.0.6-r2)
(5/5) Installing snort (2.9.11-r0)
Executing snort-2.9.11-r0.pre-install
Executing busybox-1.27.2-r7.trigger
OK: 7 MiB in 16 packages
/ #
```

Figure 115. Installing Snort after “apk update” in Alpine

11.5.1 SOME FILES ARE MISSING…

In particular, if the student installs Snort only using “apk add snort”, the following files are missing:

- All the rules (folder /etc/snort/rules). By default, this installation is storing the rules in /var/lib/snort/etc. But the rules are not there either…
- The files shown in the following figure are symbolic links to nothing. The files are missing.



```
/etc/snort # ls -la
total 40
drwxr-xr-x    3 root     root          4096 May 14 11:09 .
drwxr-xr-x    1 root     root          4096 May 14 10:07 ..
lrwxrwxrwx    1 root     root            40 May 14 10:07 classification.config -> /var/lib/snort/etc/classification.config
lrwxrwxrwx    1 root     root            35 May 14 10:07 reference.config -> /var/lib/snort/etc/reference.config
drwxr-xr-x    2 root     root          4096 May  6 23:50 rules
-rw-r--r--    1 root     root         26945 May 14 11:14 snort.conf
lrwxrwxrwx    1 root     root            33 May 14 10:07 threshold.conf -> /var/lib/snort/etc/threshold.conf
lrwxrwxrwx    1 root     root            30 May 14 10:07 unicode.map -> /var/lib/snort/etc/unicode.map
```

Figure 116. Snort in Alpine - “missing links”

So, in order to simplify the tests with Alpine, the folder “rules” and the previous missing files should be provided. The student must follow the following steps:

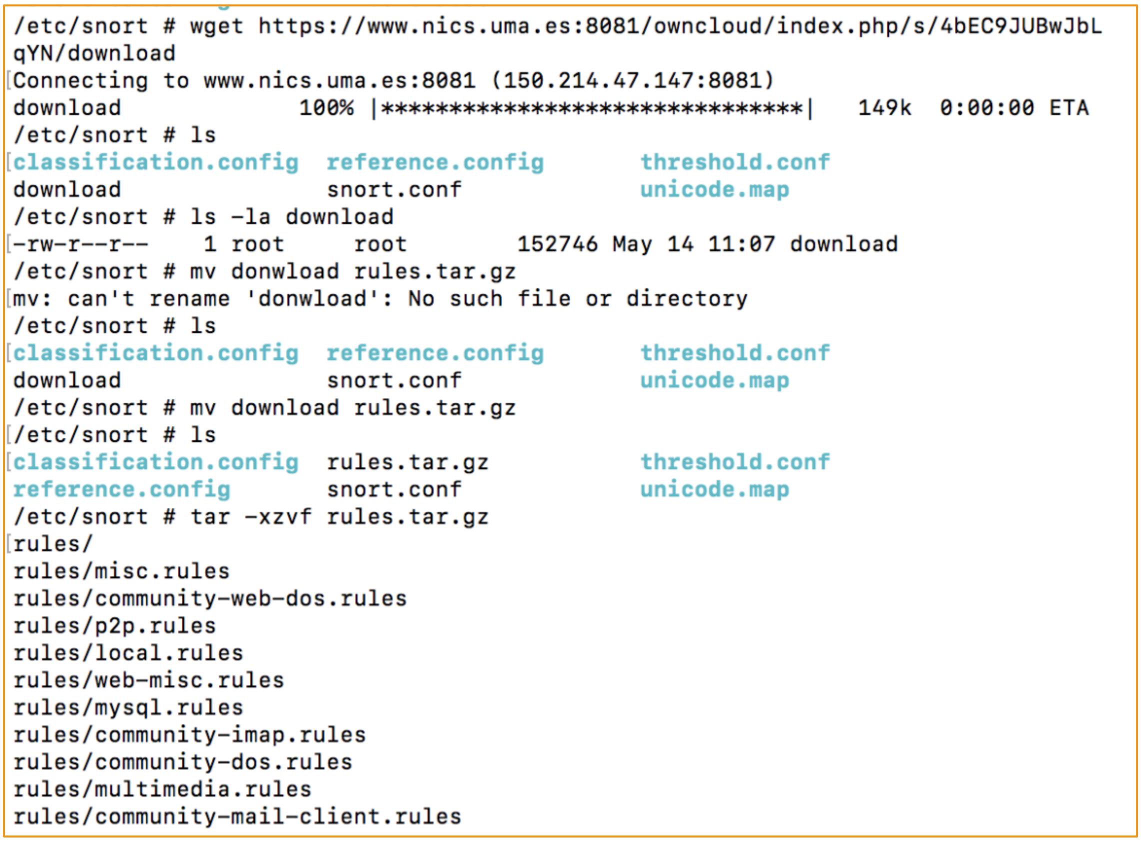
Step 1. Download, using wget the following files from Alpine, using the command-line (an example is shown in Figure 117**):**

https://www.nics.uma.es:8081/owncloud/index.php/s/4bEC9JUBwJbLqYN/download
https://www.nics.uma.es:8081/owncloud/index.php/s/MD29MeZ7MexCVUp/download

Step 2. Uncompressing the files…

- **The first file must be re-named to be the "rules" folder. Moreover, the student must configure the file *snort.conf* in order to define the PATH for the rules (/etc/snort/rules).**
- **The second files must remain in /etc/snort, such as in the Kali Linux.**

Step 3. Remove any *irrelevant rules (.rule files)* in snort.conf.



```
/etc/snort # wget https://www.nics.uma.es:8081/owncloud/index.php/s/4bEC9JUBwJbL
qYN/download
[Connecting to www.nics.uma.es:8081 (150.214.47.147:8081)
download             100% |*******************************|   149k  0:00:00 ETA
/etc/snort # ls
[classification.config  reference.config       threshold.conf
download                snort.conf             unicode.map
/etc/snort # ls -la download
[-rw-r--r--    1 root     root        152746 May 14 11:07 download
/etc/snort # mv donwload rules.tar.gz
[mv: can't rename 'donwload': No such file or directory
/etc/snort # ls
[classification.config  reference.config       threshold.conf
download                snort.conf             unicode.map
/etc/snort # mv download rules.tar.gz
[/etc/snort # ls
[classification.config  rules.tar.gz           threshold.conf
reference.config        snort.conf             unicode.map
/etc/snort # tar -xzvf rules.tar.gz
[rules/
rules/misc.rules
rules/community-web-dos.rules
rules/p2p.rules
rules/local.rules
rules/web-misc.rules
rules/mysql.rules
rules/community-imap.rules
rules/community-dos.rules
rules/multimedia.rules
rules/community-mail-client.rules
```

Figure 117. Example downloading rules using wget

After these changes, the execution of snort should work.

12 HONEYDRIVE

HoneyDrive is a honeypot Linux distro. *"Is is a virtual appliance (OVA) with Xubuntu Desktop 12.04.4 LTS edition installed. It contains over 10 pre-installed and pre-configured honeypot software packages such as:*

- *Kippo SSH honeypot,*
- *Dionaea and*
- *Amun malware honeypots,*
- *Honeyd low-interaction honeypot,*
- *Glastopf web honeypot and Wordpot,*
- *Conpot SCADA/ICS honeypot,*
- *Thug and*
- *PhoneyC honeyclients."*

This can be downloaded from the official website: *https://bruteforcelab.com/honeydrive*. Usr/Pwd: **honeydrive/honeydrive**. To use this virtual machine, VirtualBox is recommended.

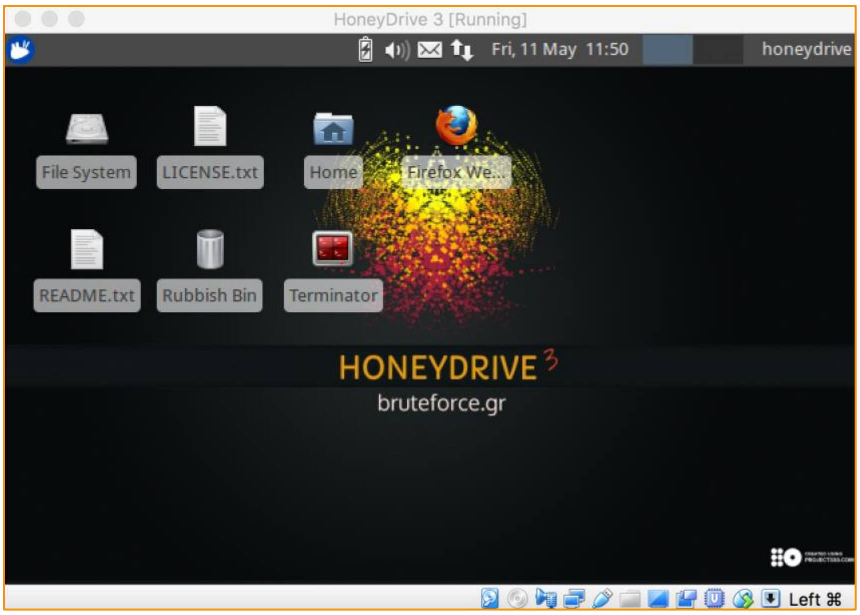


Figure 118. HoneyDrive

12.1 HONEYDRIVE IN GNS3

The first step is to connect this virtual machine to your network. Taking as an example the following network, we are going to configure HoneyDrive to be attacked.

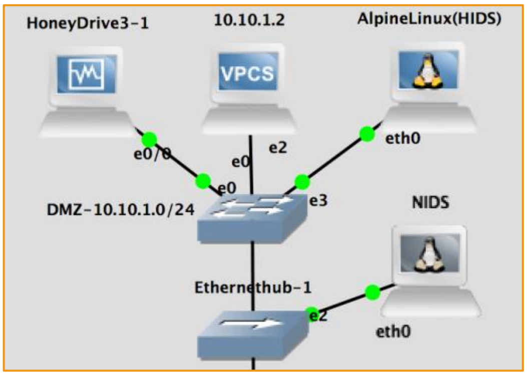
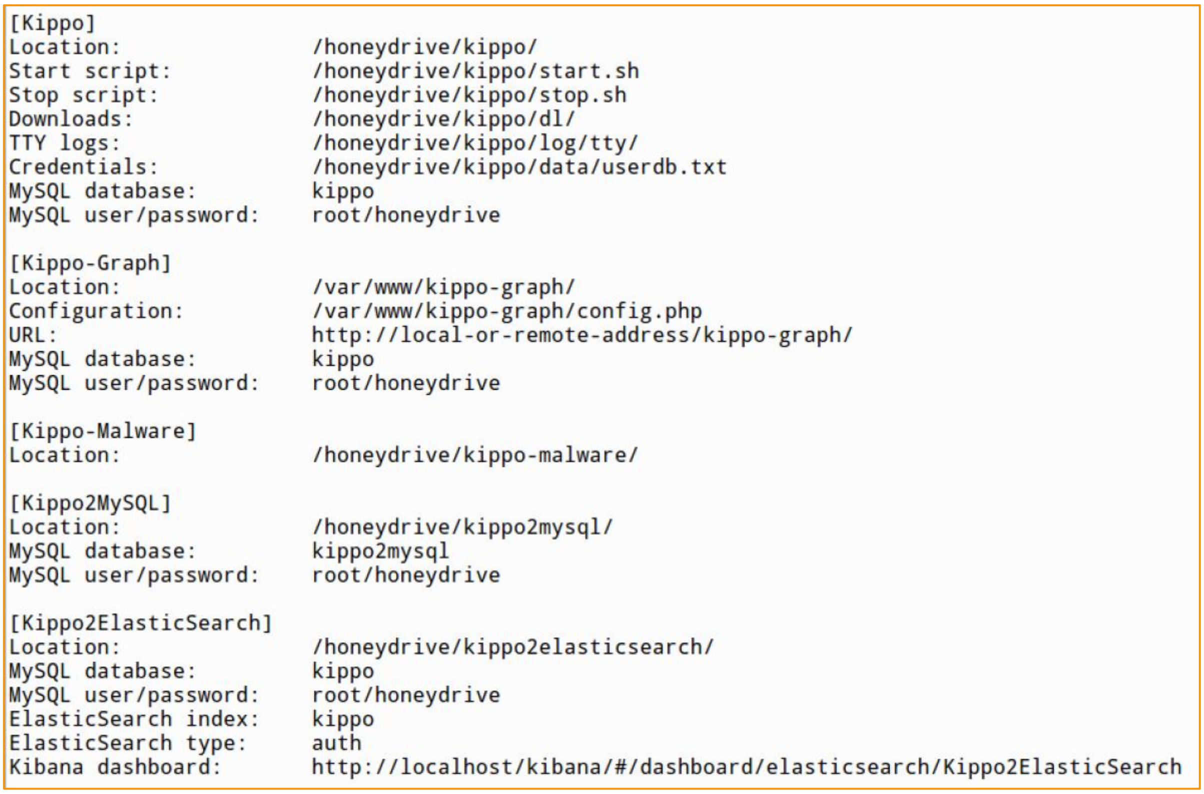


Figure 119. Honeydrive in GNS3

12.2 WHERE IS THE INFORMATION ABOUT THE HONEYPOTS?

In the Desktop, the file README.txt contains the paths and commands of the honeypots installed.



```
[Kippo]
Location:                /honeydrive/kippo/
Start script:            /honeydrive/kippo/start.sh
Stop script:             /honeydrive/kippo/stop.sh
Downloads:               /honeydrive/kippo/dl/
TTY logs:                /honeydrive/kippo/log/tty/
Credentials:             /honeydrive/kippo/data/userdb.txt
MySQL database:          kippo
MySQL user/password:     root/honeydrive

[Kippo-Graph]
Location:                /var/www/kippo-graph/
Configuration:           /var/www/kippo-graph/config.php
URL:                     http://local-or-remote-address/kippo-graph/
MySQL database:          kippo
MySQL user/password:     root/honeydrive

[Kippo-Malware]
Location:                /honeydrive/kippo-malware/

[Kippo2MySQL]
Location:                /honeydrive/kippo2mysql/
MySQL database:          kippo2mysql
MySQL user/password:     root/honeydrive

[Kippo2ElasticSearch]
Location:                /honeydrive/kippo2elasticsearch/
MySQL database:          kippo
MySQL user/password:     root/honeydrive
ElasticSearch index:     kippo
ElasticSearch type:      auth
Kibana dashboard:        http://localhost/kibana/#/dashboard/elasticsearch/Kippo2ElasticSearch
```

Figure 120. Honeydrive - A portion of the README.txt file

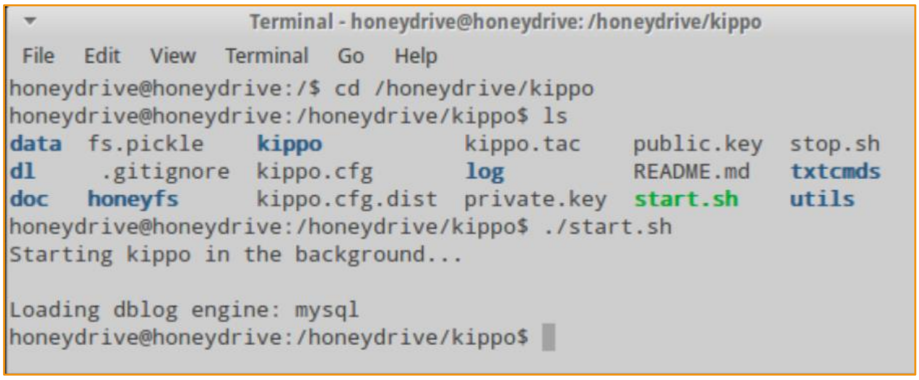
12.3 USE CASE WITH KIPPO

Kippo is a honeypot very simple to use. However, the student must consider that modern versions of ssh have problems to connect with Kippo. Therefore, in order to practise using Kali as the “attacker”, the student must install “putty” in Kali Linux (apt-get install putty).

12.3.1SETTING UP KIPPO

For example, the following steps are needed in order to launch Kippo:

1. Go to the directory for Kippo: “**cd /honeydrive/kippo/**”
2. Start Kippo: **“/honeydrive/kippo/start.h”**



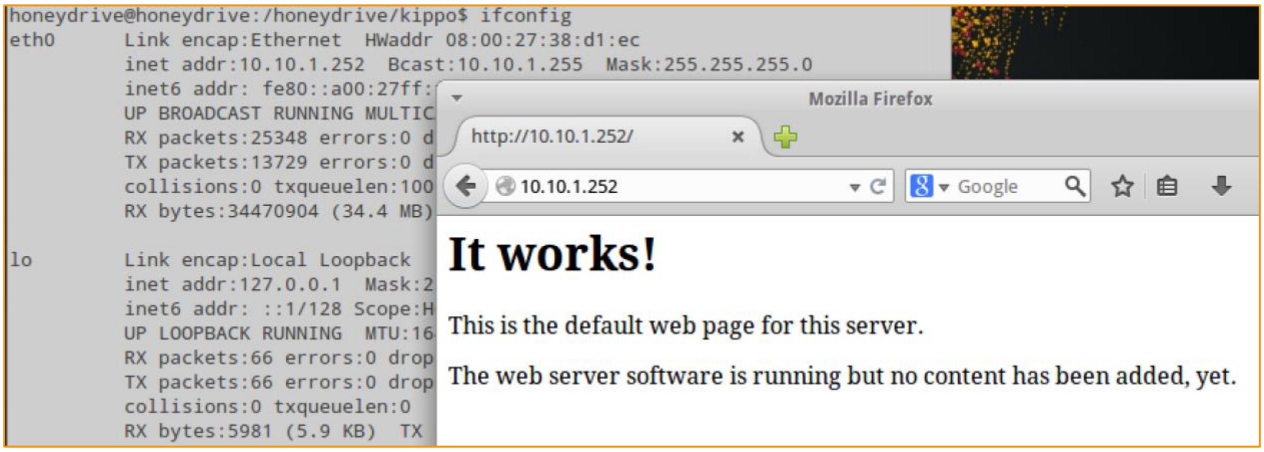
Terminal - honeydrive@honeydrive: /honeydrive/kippo
File Edit View Terminal Go Help

```
honeydrive@honeydrive:/$ cd /honeydrive/kippo
honeydrive@honeydrive:/honeydrive/kippo$ ls
data  fs.pickle   kippo          kippo.tac    public.key  stop.sh
dl     .gitignore kippo.cfg      log          README.md   txtcmds
doc   honeyfs     kippo.cfg.dist private.key  start.sh    utils
honeydrive@honeydrive:/honeydrive/kippo$ ./start.sh
Starting kippo in the background...

Loading dblog engine: mysql
honeydrive@honeydrive:/honeydrive/kippo$
```

Figure 121. Launching Kippo in Honeydrive

Then, to check if Kippo has been launched:

1. Find the IP of the virtual honeypot: **"ifconfig"**
2. Load the IP in the browser. Then, the next page should be shown.



```
honeydrive@honeydrive:/honeydrive/kippo$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:38:d1:ec
          inet addr:10.10.1.252  Bcast:10.10.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:
          UP BROADCAST RUNNING MULTIC
          RX packets:25348 errors:0 d
          TX packets:13729 errors:0 d
          collisions:0 txqueuelen:100
          RX bytes:34470904 (34.4 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:2
          inet6 addr: ::1/128 Scope:H
          UP LOOPBACK RUNNING  MTU:16
          RX packets:66 errors:0 drop
          TX packets:66 errors:0 drop
          collisions:0 txqueuelen:0
          RX bytes:5981 (5.9 KB)  TX
```

It works!

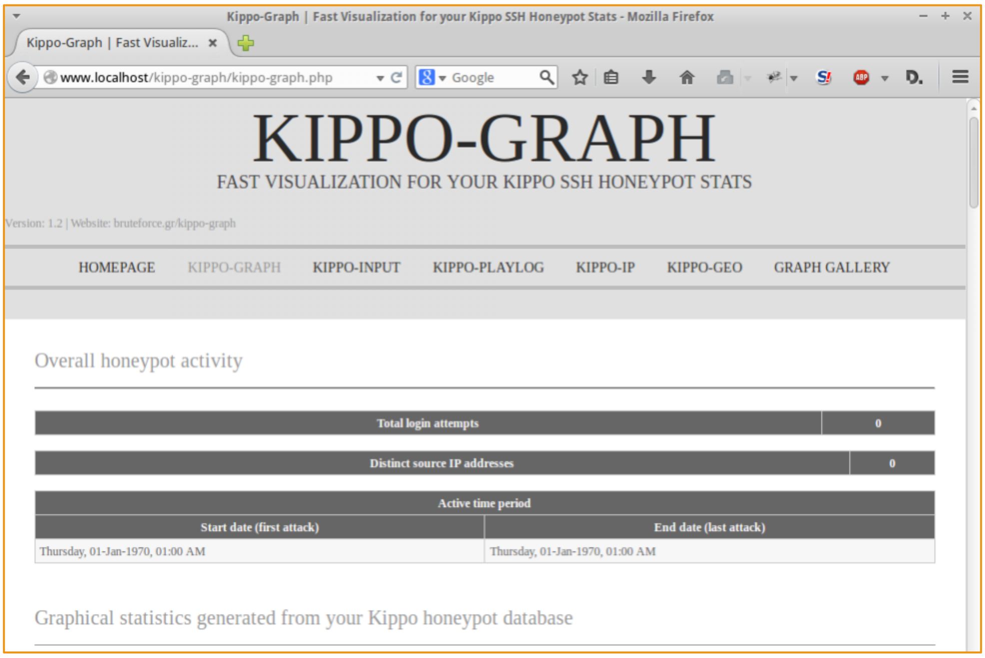
This is the default web page for this server.

The web server software is running but no content has been added, yet.

Figure 122. Honeydrive IP - Kippo IP & Kippo working

12.3.2VISUALIZE ATTACKS AGAINST KIPPO

Once Kippo has been launched, the student can monitor the activity against the honeypot using **Kippo Graph**. The URL to see the Kippo Graph is shown in the file README.txt. The student must change the text in "local-or-remote-address" by the IP of Honeydrive or "localhost" if this will be opened in the Honeydrive VM.



Kippo-Graph | Fast Visualization for your Kippo SSH Honeypot Stats - Mozilla Firefox
Kippo-Graph | Fast Visualiz...
www.localhost/kippo-graph/kippo-graph.php
Google

KIPPO-GRAPH

FAST VISUALIZATION FOR YOUR KIPPO SSH HONEYPOT STATS

Version: 1.2 | Website: bruteforce.gr/kippo-graph

HOMEPAGE
KIPPO-GRAPH
KIPPO-INPUT
KIPPO-PLAYLOG
KIPPO-IP
KIPPO-GEO
GRAPH GALLERY

Overall honeypot activity

Total login attempts	0

Distinct source IP addresses	0

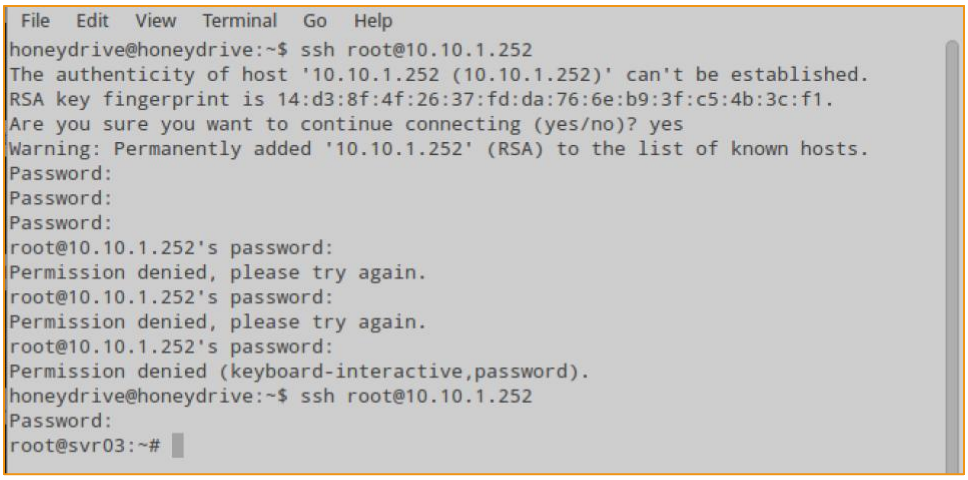
Active time period	
Start date (first attack)	End date (last attack)
Thursday, 01-Jan-1970, 01:00 AM	Thursday, 01-Jan-1970, 01:00 AM

Graphical statistics generated from your Kippo honeypot database

Figure 123.Kippo-Graph

12.3.3 TESTING KIPPO

In order to check Kippo, the student can connect by ssh to the IP of the Kippo machine. Try to login as root.



```
honeydrive@honeydrive:~$ ssh root@10.10.1.252
The authenticity of host '10.10.1.252 (10.10.1.252)' can't be established.
RSA key fingerprint is 14:d3:8f:4f:26:37:fd:da:76:6e:b9:3f:c5:4b:3c:f1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.1.252' (RSA) to the list of known hosts.
Password:
Password:
Password:
root@10.10.1.252's password:
Permission denied, please try again.
root@10.10.1.252's password:
Permission denied, please try again.
root@10.10.1.252's password:
Permission denied (keyboard-interactive,password).
honeydrive@honeydrive:~$ ssh root@10.10.1.252
Password:
root@svr03:~#
```

Figure 124. Testing Kippo

The following picture shows the results after various logins from the Kali Linux (using putty).

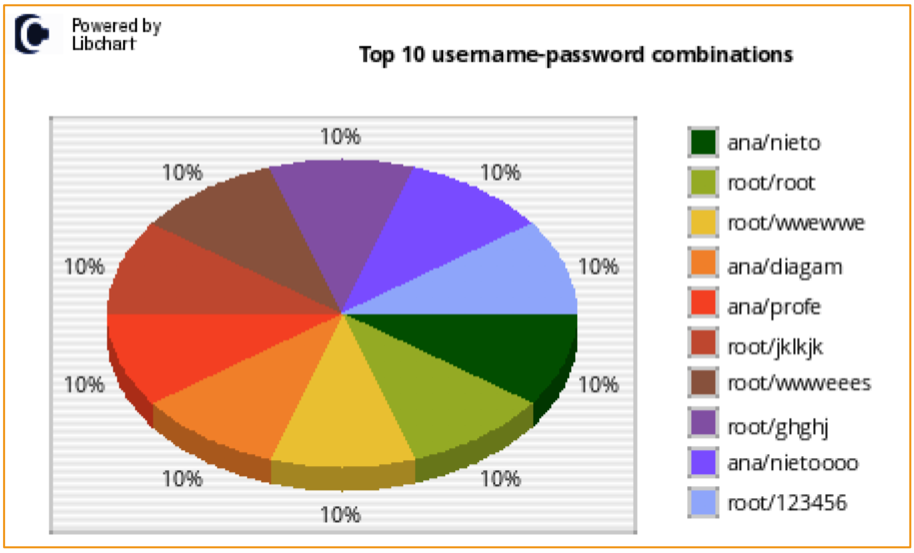


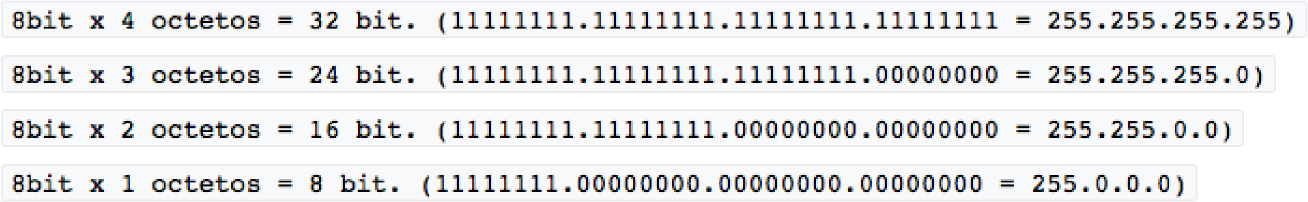
Figure 125. Results shown using Kippo-Graph

13 GENERAL CONCEPTS

13.1 NETWORK MASK

2_8= 256. This means that using 8 bits you can represent 256 elements.

The following picture represents a set of typical network masks to express network ranges. For example, note that I0.10.10.1/32 means that only the IP==10.10.10.1 satisfies the requirements to be part of the network.

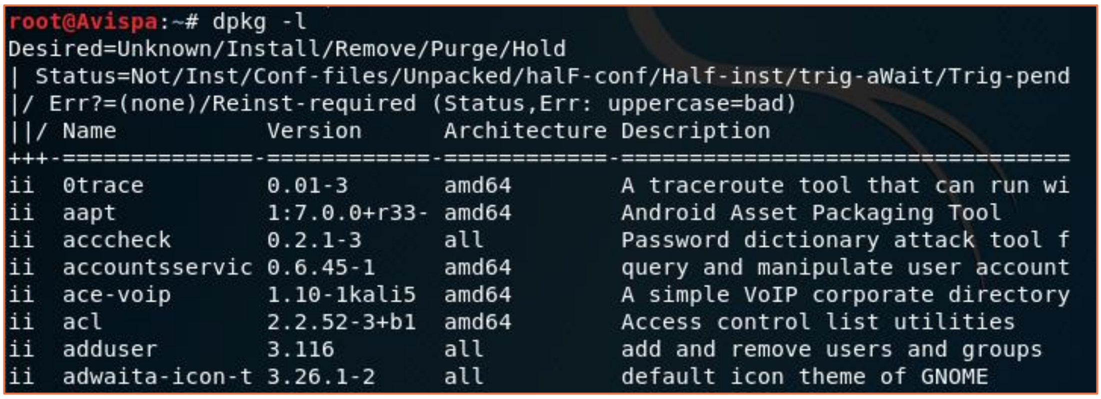


```
8bit x 4 octetos = 32 bit. (11111111.11111111.11111111.11111111 = 255.255.255.255)

8bit x 3 octetos = 24 bit. (11111111.11111111.11111111.00000000 = 255.255.255.0)

8bit x 2 octetos = 16 bit. (11111111.11111111.00000000.00000000 = 255.255.0.0)

8bit x 1 octetos = 8 bit. (11111111.00000000.00000000.00000000 = 255.0.0.0)
```

Figure 126. Typical network masks

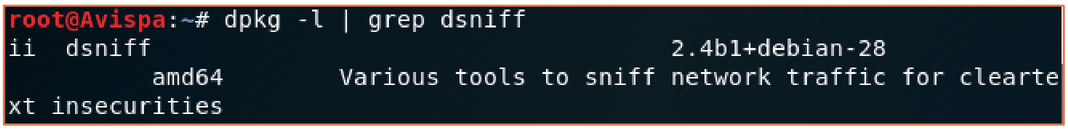
13.2 CHECK IF A PACKET IS INSTALLED IN KALI (DEBIAN / UBUNTU IN GENERAL)

"*dpkg -l*" lists the packets already installed in the machine. "*dpkg -l | grep dsniff*" list the information about packets which contains "dsniff" in the name.



```
root@Avispa:~# dpkg -l
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name           Version      Architecture Description
+++-==============-============-============-=================================
ii  0trace         0.01-3       amd64        A traceroute tool that can run wi
ii  aapt           1:7.0.0+r33- amd64        Android Asset Packaging Tool
ii  acccheck       0.2.1-3      all          Password dictionary attack tool f
ii  accountsservic 0.6.45-1     amd64        query and manipulate user account
ii  ace-voip       1.10-1kali5  amd64        A simple VoIP corporate directory
ii  acl            2.2.52-3+b1  amd64        Access control list utilities
ii  adduser        3.116        all          add and remove users and groups
ii  adwaita-icon-t 3.26.1-2     all          default icon theme of GNOME
```

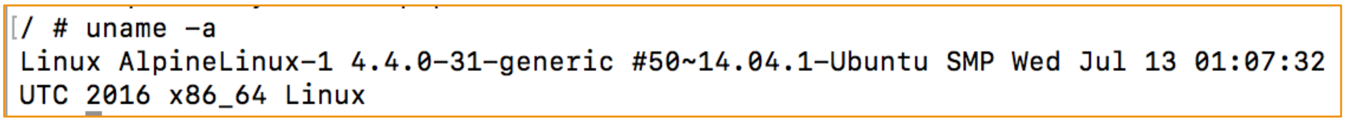
Figure 127. List of packets installed in Kali



```
root@Avispa:~# dpkg -l | grep dsniff
ii  dsniff                                    2.4b1+debian-28
         amd64        Various tools to sniff network traffic for clearte
xt insecurities
```

Figure 128. List of packets with "dsniff"

13.3 CHECK THE VERSION OF A LINUX OPERATING SYSTEM FROM THE COMMAND-LINE

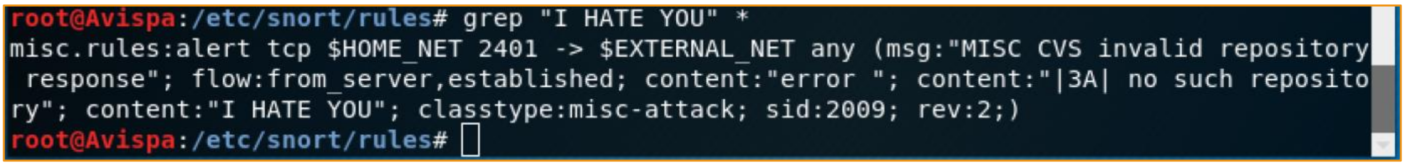


```
/ # uname -a
Linux AlpineLinux-1 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:07:32
UTC 2016 x86_64 Linux
```

Figure 129. Check the version of a Linux Operating System

13.4 FIND A FILE WHICH CONTAINS A STRING

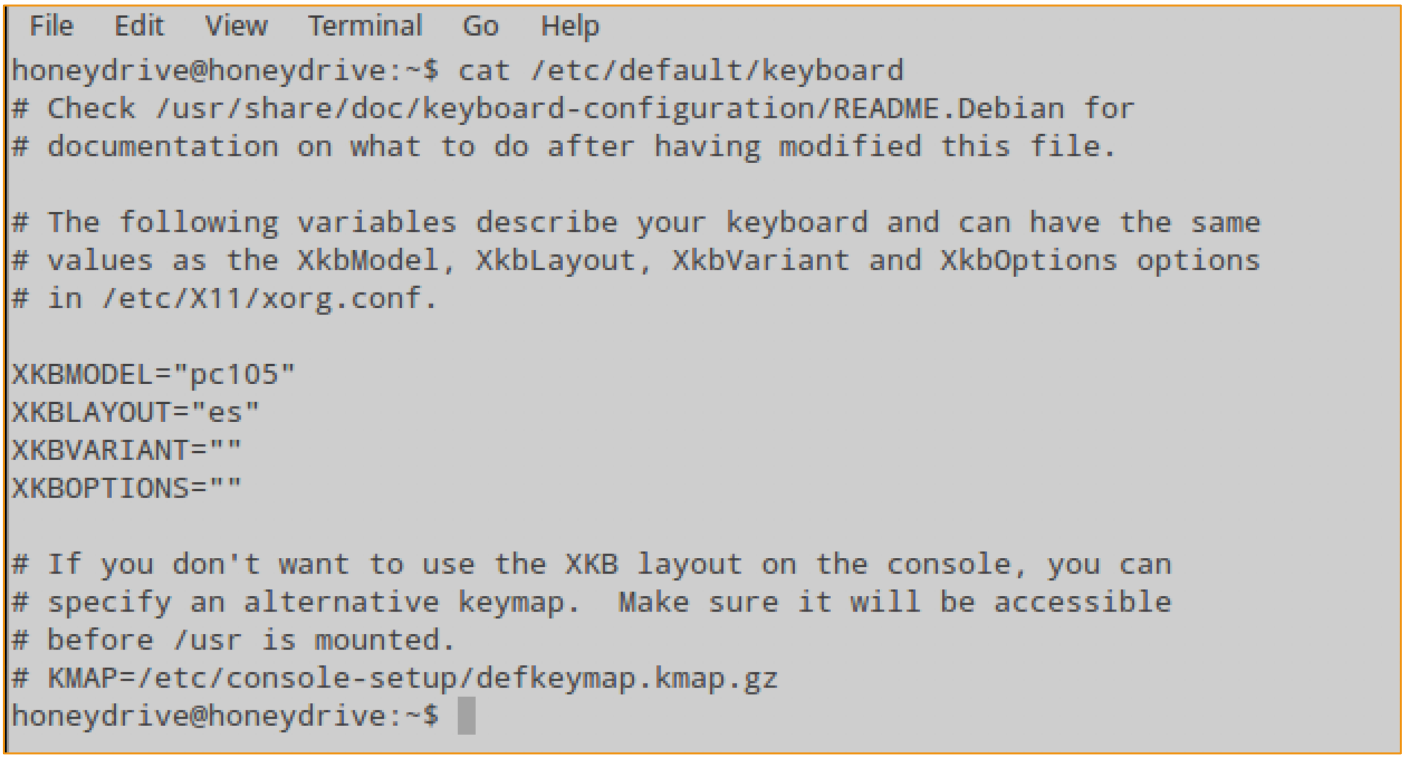
The following figure shows how the command **grep** can be used to find the name of the file which contains the string "I HATE YOU". Note that the result not only shows the name of the file (misc.rules), but also shows the line in which the string appears.



```
root@Avispa:/etc/snort/rules# grep "I HATE YOU" *
misc.rules:alert tcp $HOME_NET 2401 -> $EXTERNAL_NET any (msg:"MISC CVS invalid repository
 response"; flow:from_server,established; content:"error "; content:"|3A| no such reposito
ry"; content:"I HATE YOU"; classtype:misc-attack; sid:2009; rev:2;)
root@Avispa:/etc/snort/rules# 
```

Figure 130. Find the name of the file which contains the string "I HATE YOU"

13.5 CHANGE THE KEYBOARD LANGUAGE IN UBUNTU



```
honeydrive@honeydrive:~$ cat /etc/default/keyboard
# Check /usr/share/doc/keyboard-configuration/README.Debian for
# documentation on what to do after having modified this file.

# The following variables describe your keyboard and can have the same
# values as the XkbModel, XkbLayout, XkbVariant and XkbOptions options
# in /etc/X11/xorg.conf.

XKBMODEL="pc105"
XKBLAYOUT="es"
XKBVARIANT=""
XKBOPTIONS=""

# If you don't want to use the XKB layout on the console, you can
# specify an alternative keymap.  Make sure it will be accessible
# before /usr is mounted.
# KMAP=/etc/console-setup/defkeymap.kmap.gz
honeydrive@honeydrive:~$
```

Figure 131. Ubuntu - Change keyboard language