Étape 1 : Découverte du pare-feu

Q1. A partir de la station **pirate3** située dans l'Internet, veuillez découvrir la passerelle du réseau local cible.

```
root@pirate3:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 0c:d3:a7:ff:91:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.242/24 brd 192.168.122.255 scope global dynamic eth0
       valid_lft 3021sec preferred_lft 3021sec
    inet6 fe80::ed3:a7ff:feff:9100/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 0c:d3:a7:ff:91:01 brd ff:ff:ff:ff:ff:ff
root@pirate3:~# nmap -sn 192.168.122.242
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-02 08:00 UTC
Nmap scan report for pirate3 (192.168.122.242)
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
```

Q2. Quels sont les ports ouverts sur cette cible ?

```
root@pirate3:~# nmap -sn 192.168.122.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-02 08:03 UTC
Nmap scan report for capgchamb4 (192.168.122.1)
Host is up (0.00097s latency).
MAC Address: 52:54:00:9C:B2:69 (QEMU virtual NIC)
Nmap scan report for vulnscan (192.168.122.7)
Host is up (0.0023s latency).
MAC Address: 0C:D3:A7:1D:E0:00 (Unknown)
Nmap scan report for 192.168.122.122
Host is up (0.00076s latency).
MAC Address: 0C:D3:A7:7D:69:01 (Unknown)
Nmap scan report for controller (192.168.122.124)
Host is up (0.0016s latency).
MAC Address: 0C:D3:A7:C5:B9:01 (Unknown)
Nmap scan report for R1 (192.168.122.221)
Host is up (0.0017s latency).
MAC Address: 0C:D3:A7:A6:6E:01 (Unknown)
Nmap scan report for pirate3 (192.168.122.242)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 1.59 seconds
root@pirate3:~#
```

On voit que les ports 22 (TCP) et 8000 (TCP) sont ouverts.

```
root@pirate3:~# nmap 192.168.122.122
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-02 08:09 UTC
Stats: 0:00:22 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 63.65% done; ETC: 08:09 (0:00:13 remaining)
Nmap scan report for 192.168.122.122
Host is up (0.00070s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
8000/tcp open  http-alt
MAC Address: 0C:D3:A7:7D:69:01 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 38.32 seconds
root@pirate3:~#
```

Q3. Comment pouvez-vous découvrir l'implémentation des protocoles que vous avez trouvés ? *En essayant d'établir une connexion via ces ports.*

Q4. Veuillez-vous connecter à partir de la station pirate sur la cible avec un login *root* et un mot de passe faible comme *testtest*.

On se connecte en SSH sur le pare-feu :

```
root@pirate3:~# ssh root@192.168.122.122
root@192.168.122.122's password:


BusyBox v1.23.2 (2016-01-02 12:56:51 CET) built-in shell (ash)

  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 -----------------------------------------------------
 CHAOS CALMER (15.05.1, r48532)
 -----------------------------------------------------
  * 1 1/2 oz Gin             Shake with a glassful
  * 1/4 oz Triple Sec        of broken ice and pour
  * 3/4 oz Lime Juice        unstrained into a goblet.
  * 1 1/2 oz Orange Juice
  * 1 tsp. Grenadine Syrup
 -----------------------------------------------------
root@OpenWrt:~#
```

Étape 2 : Découverte interne

Q1. Veuillez identifier le seul ordinateur de ce réseau qui ne dispose pas de nom inverse à son adresse IP ?

L'adresse locale de pirate2 est 192.186.99.186 /24. L'adresse du réseau dans lequel se trouve le pirate est 192.168.99.0

```
root@pirate2:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 0c:d3:a7:84:35:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.99.186/24 brd 192.168.99.255 scope global dynamic eth0
       valid_lft 37314sec preferred_lft 37314sec
    inet6 fd38:1a54:16e2::80f/128 scope global noprefixroute
       valid_lft forever preferred_lft forever
    inet6 fd38:1a54:16e2:0:ed3:a7ff:fe84:3500/64 scope global mngtmpaddr noprefixroute
       valid_lft forever preferred_lft forever
    inet6 fe80::ed3:a7ff:fe84:3500/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 0c:d3:a7:84:35:01 brd ff:ff:ff:ff:ff:ff
```

```
root@pirate2:~# arp-scan 192.168.99.0/24
Interface: eth0, type: EN10MB, MAC: 0c:d3:a7:84:35:00, IPv4: 192.168.99.186
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.99.1    0c:d3:a7:7d:69:00       (Unknown)
192.168.99.130  0c:d3:a7:2b:a3:00       (Unknown)
192.168.99.146  0c:d3:a7:7a:12:00       (Unknown)
192.168.99.166  0c:d3:a7:1b:49:00       (Unknown)
192.168.99.172  0c:d3:a7:5b:91:00       (Unknown)

5 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.284 seconds (112.08 hosts/sec). 5 responded
root@pirate2:~#
```

L'ordinateur qui ne pose pas de nom inverse à son adresse IP est celui possède l'adresse IP 192.168.99.172

```
root@pirate2:~# nmap -sn 192.168.99.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-02 09:28 UTC
Nmap scan report for OpenWrt.lan (192.168.99.1)
Host is up (0.0012s latency).
MAC Address: 0C:D3:A7:7D:69:00 (Unknown)
Nmap scan report for WIN-JBJ87HGI36A.lan (192.168.99.130)
Host is up (0.0015s latency).
MAC Address: 0C:D3:A7:2B:A3:00 (Unknown)
Nmap scan report for pirate1.lan (192.168.99.146)
Host is up (0.0031s latency).
MAC Address: 0C:D3:A7:7A:12:00 (Unknown)
Nmap scan report for ie8winxp.lan (192.168.99.166)
Host is up (0.0011s latency).
MAC Address: 0C:D3:A7:1B:49:00 (Unknown)
Nmap scan report for 192.168.99.172
Host is up (0.0031s latency).
MAC Address: 0C:D3:A7:5B:91:00 (Unknown)
Nmap scan report for pirate2.lan (192.168.99.186)
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 1.63 seconds
root@pirate2:~#
```

Q2. Veuillez-vous intéresser aux ports du protocole ancestral non sécurisé RSH. Quels sont-ils ? Veuillez-vous connecter en RSH avec un compte *root* sur cette cible (apt install rsh-client au préalable).

Les ports liés au protocole RSH sont les ports 512 (Rexec), 513 (Rlogin) et 514 (RSHell).

```
root@pirate2:~# nmap 192.168.99.172
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-02 09:36 UTC
Nmap scan report for 192.168.99.172
Host is up (0.00093s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 0C:D3:A7:5B:91:00 (Unknown)
```

Connexion en RSH sur la cible :

```
root@pirate2:~# rsh -l root 192.168.99.172
Last login: Thu Apr  2 03:46:52 EDT 2020 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~#
```

Q3. Quels sont les autres protocoles qui permettraient d'exploiter des consoles ?

En faisant nmap 192.168.99.172, on observe beaucoup de ports ouverts :

```
root@pirate2:~# nmap 192.168.99.172
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-02 09:36 UTC
Nmap scan report for 192.168.99.172
Host is up (0.00093s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 0C:D3:A7:5B:91:00 (Unknown)
```

On peut donc essayer de se connecter en telnet, ssh, ftp …

Q4. En sachant qu'un compte msfadmin est configuré avec un mot de passe faible, veuillez exploiter l'un de ces protocoles.

Les login et mot de passe sont msfadmin

Exemple de connexion en Telnet :

```
root@pirate2:~# telnet 192.168.99.172
Trying 192.168.99.172...
Connected to 192.168.99.172.
Escape character is '^]'.
                  _                  _       _ _                 _     _       ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Wed Feb  1 16:17:51 EST 2017 on ttyS0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Exemple de connexion en SSH :

```
root@pirate2:~# ssh msfadmin@192.168.99.172
The authenticity of host '192.168.99.172 (192.168.99.172)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.99.172' (RSA) to the list of known hosts.
msfadmin@192.168.99.172's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Thu Apr  2 05:58:17 2020 from pirate2.lan
msfadmin@metasploitable:~$
```

Étape 3 : découverte de vulnérabilités

Q1. Quel est la nature de la vulnérabilité du premier service découvert ?

nmap --script vuln 192.168.99.172
Cette commande prend environ 5 min à aboutir. On obtient un scan des vulnérabilités de la cible 192.168.99.172

```
root@pirate2:~# nmap --script vuln 192.168.99.172
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-02 10:10 UTC
```

Extrait du rapport de vulnérabilités :

```
root@pirate2:~# nmap --script vuln 192.168.99.172
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-02 10:10 UTC
Stats: 0:04:03 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.81% done; ETC: 10:14 (0:00:00 remaining)
Nmap scan report for 192.168.99.172
Host is up (0.0011s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp <--
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://www.securityfocus.com/bid/48539
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234
_backdoor.rb
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_sslv2-drown:
22/tcp   open  ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
23/tcp   open  telnet
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
25/tcp   open  smtp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
```

Le premier service vulnérable trouvé est le service FTP sur le port TCP 21.

Q2. Pouvez-vous fournir une procédure d'exploitation réalisable avec Kali Linux (par exemple, si autre préciser) de manière manuelle, avec metasploit ou un binaire dédié ?
Il faut aller se documenter sur la procédure en utilisant les références fournies dans le rapport de vulnérabilités obtenu à la question 1.

```
21/tcp   open  ftp
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://www.securityfocus.com/bid/48539
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_sslv2-drown:
```

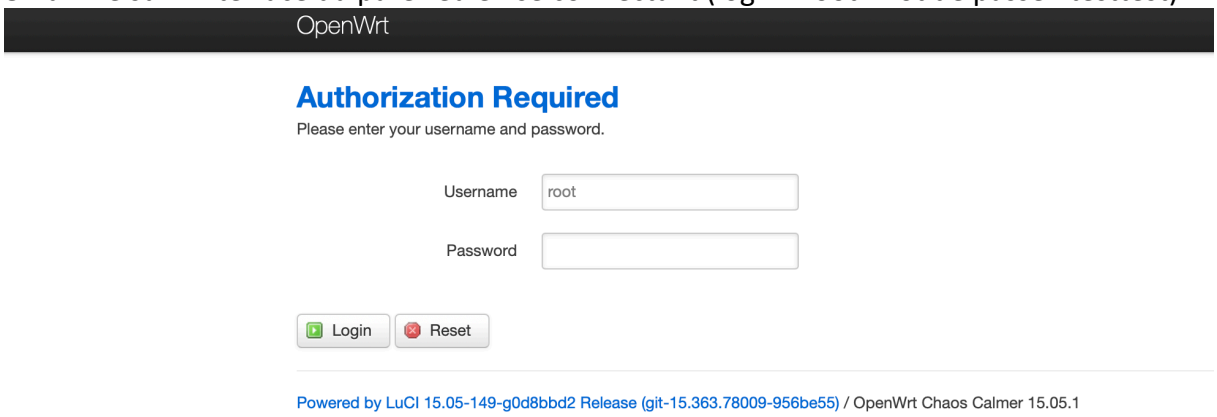
Q3. Quels sont les services qui comportent le plus de vulnérabilités ?
Q4. Quel est le framework qui permettrait d'auditer et de fournir des contre-mesures à ces vulnérabilités remarquables ?

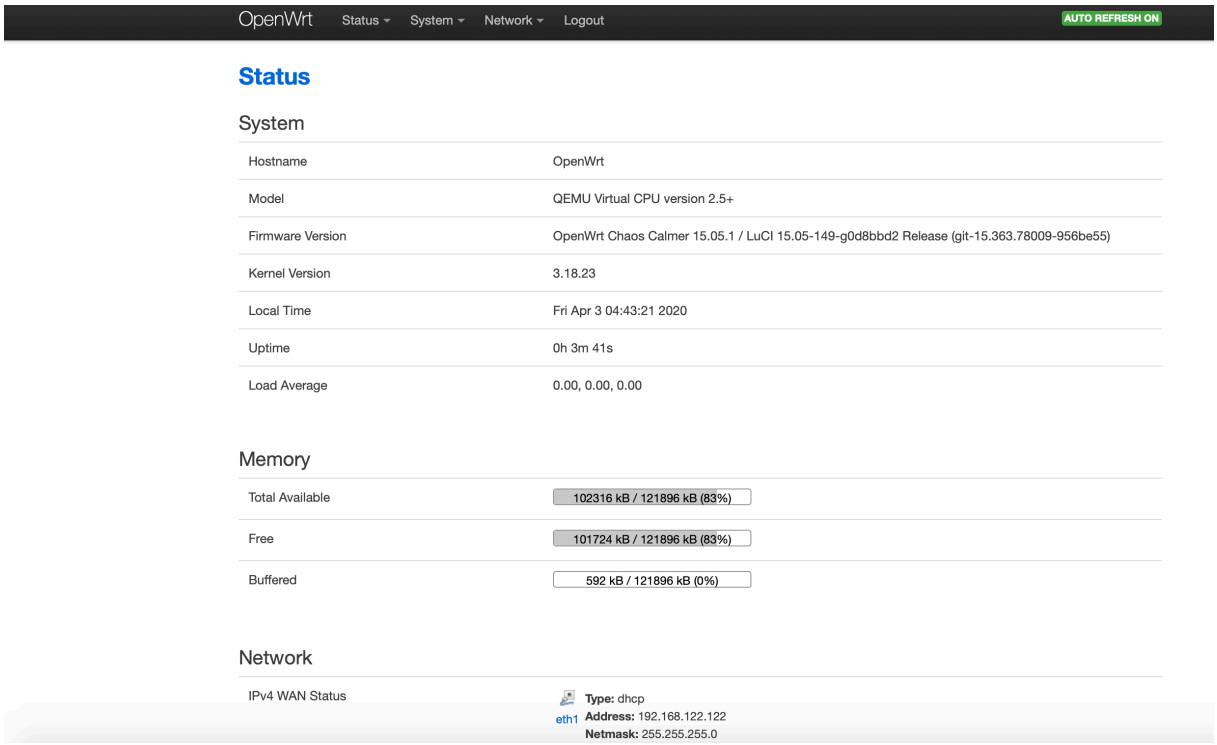
OWASP Top Ten : recense le top 10 des vulnérabilités sur lesquelles il faut se focaliser.

Étape 4 : Analyse des règles du pare-feu

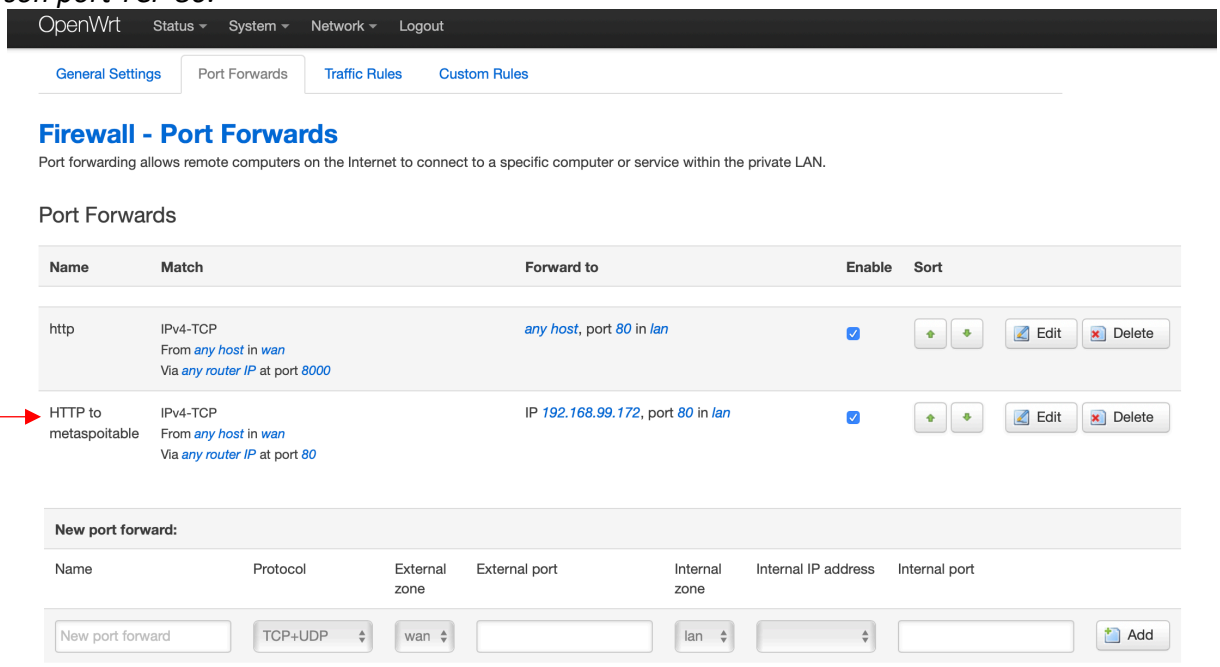
Le pare-feu est maintenant accessible depuis mon ordinateur en http :

On arrive sur l'interface du pare-feu en se connectant (login : root mot de passe : testtest)





Transfert du port TCP 80 sur le WAN vers la cible (192.168.99.72 : machine mtaspoiltable) sur son port TCP 80.



Depuis mon ordinateur, j'accède au serveur http de la cible (machine metasploitable) :

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

Étape 5 : le pare-feu n'est pas une sécurité

On désactive le pare-feu de la passerelle mais on maintient le NAT :

```
root@OpenWrt:/# iptables -t filter -F
root@OpenWrt:/# iptables -t filter -X
root@OpenWrt:/# iptables -t filter -A FORWARD -j ACCEPT
root@OpenWrt:/# iptables -t filter -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@OpenWrt:/#
```

```
msfadmin@metasploitable:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 0c:d3:a7:5b:91:00
          inet addr:192.168.99.172  Bcast:192.168.99.255  Mask:255.255.255.0
          inet6 addr: fd38:1a54:16e2:0:ed3:a7ff:fe5b:9100/64 Scope:Global
          inet6 addr: fe80::ed3:a7ff:fe5b:9100/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:199 errors:87 dropped:0 overruns:0 frame:87
          TX packets:122 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:27124 (26.4 KB)  TX bytes:16249 (15.8 KB)
          Base address:0xc000 Memory:feb80000-feba0000

msfadmin@metasploitable:~$
```

On fait un ping sur une adresse publique :

```
msfadmin@metasploitable:~$ ping -c1 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=56 time=7.83 ms

--- 1.1.1.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 7.838/7.838/7.838/0.000 ms
msfadmin@metasploitable:~$
```

Le ping fonctionne correctement : cela signifie qu'on parvient à joindre l'internet avec un pare-feu désactivé et un NAT maintenu.

LE NAT NE PROTÈGE PAS.

```
root@pirate3:~# ip route
default via 192.168.122.1 dev eth0 proto dhcp src 192.168.122.242 metric 100
192.168.122.0/24 dev eth0 proto kernel scope link src 192.168.122.242
192.168.122.1 dev eth0 proto dhcp scope link src 192.168.122.242 metric 100
root@pirate3:~#
```

On ajoute une route IP dans le LAN privé de destination :

```
root@pirate3:~# ip route add 192.168.99.0/24 via 192.168.122.122 dev eth0
root@pirate3:~# ip route
default via 192.168.122.1 dev eth0 proto dhcp src 192.168.122.242 metric 100
192.168.99.0/24 via 192.168.122.122 dev eth0
192.168.122.0/24 dev eth0 proto kernel scope link src 192.168.122.242
192.168.122.1 dev eth0 proto dhcp scope link src 192.168.122.242 metric 100
root@pirate3:~#
```

On vérifie la connectivité entre le pirate3 et la cible (192.168.99.172) :

```
root@pirate3:~# ping -c1 192.168.99.172
PING 192.168.99.172 (192.168.99.172) 56(84) bytes of data.
64 bytes from 192.168.99.172: icmp_seq=1 ttl=63 time=14.2 ms

--- 192.168.99.172 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 14.244/14.244/14.244/0.000 ms
root@pirate3:~#
```

Le pirate arrive bien à joindre sa cible (metasploitable) depuis l'internet.