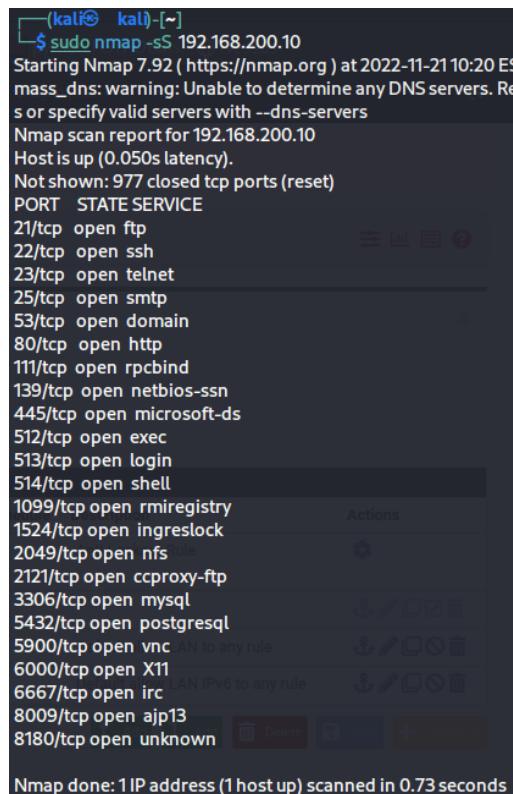
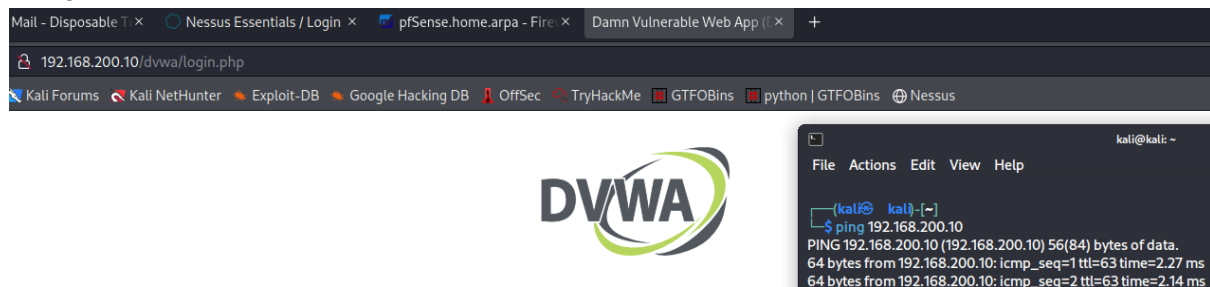


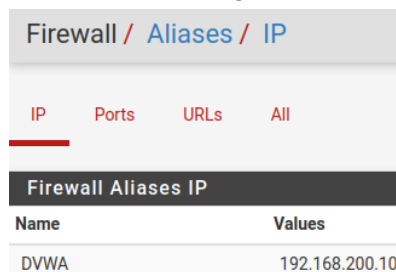
# CONFIGURAZIONE FIREWALL PFSENSE

Bisogna bloccare il DVWA dall'ip di metasploit tramite pfsense.



qui funziona da kali, nmap

Ora creiamo la regola nel firewall



ho creato un Alias nominato DVWA corrispondente all'IP

Firewall / Rules / Edit

### Edit Firewall Rule

**Action** Block

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

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

**Interface** LAN

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

**Address Family** IPv4

Select the Internet Protocol version this rule applies to.

**Protocol** TCP

Choose which IP protocol this rule should match.

#### Source

**Source** ☐ Invert match any Source Address /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

#### Destination

**Destination** ☐ Invert match Single host or alias DVWA /

**Destination Port Range** HTTP (80)  HTTPS (443)

From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

qui la regola del firewall con specificato l'azione blocca, l'alias e il range di porte. Qui da 80 a 443 per bloccare tutti gli accessi eventuali web.

Sotto lo screen di nmap mancanti le porte 80-443

```
(kali㉿ kali) [~]
$ sudo nmap -sS 192.168.200.10
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 10:19 EST
mass_dns: warning: Unable to determine any DNS servers. Rev
-system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.200.10
Host is up (0.013s latency).
Not shown: 931 closed tcp ports (reset), 49 filtered tcp ports (no
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
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

Nmap done: 1 IP address (1 host up) scanned in 1.89 seconds
```