Università degli Studi di Salerno

Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Configurazione Ambiente per il Corso di Penetration Testing

Arcangelo Castiglione
arcastiglione@unisa.it

Outline

- Ambiente Operativo
- Asset Vulnerabili
- Architettura di Rete

Outline

- **Ambiente Operativo**
- Asset Vulnerabili
- Architettura di Rete

Ambiente Operativo

Motivazioni

- Ambiente all'interno del quale poter sperimentare e praticare l'Ethical Hacking

- Permette di **esercitarsi** sugli argomenti mostrati al corso
  - **Senza** incorrere in **rischi** né di carattere **tecnico** né di carattere **legale**

Ambiente Operativo

Motivazioni

- Utilizzeremo un **ambiente operativo «controllato»**
  - Invece di utilizzare servizi vulnerabili in ambienti reali presenti sulla rete Internet
- Obiettivi
  - Migliorare le proprie abilità in maniera controllata
  - Acquisire conoscenza senza né violare alcuna legge né mettere fuori uso sistemi

Ambiente Operativo

Motivazioni

- Vantaggi
  - Se qualcosa non dovesse andare a buon fine sarebbe più facile risolvere problemi e capire cosa sta accadendo sul sistema analizzato
  - Se accadesse qualcosa al sistema operativo eseguito in macchina virtuale potremmo ripristinarlo più facilmente
    - Ad esempio, utilizzando le **Istantanee** di VirtualBox

Ambiente Operativo

Declinazione di Responsabilità

- **Mai effettuare attività di penetration testing su macchine al di fuori dell'ambiente operativo del corso**
  - **Senza adeguata e preventiva autorizzazione (scritta)**

- **In diversi paesi, anche il solo *port scanning* non autorizzato su una macchina può essere considerato un atto criminale**

Ambiente Operativo

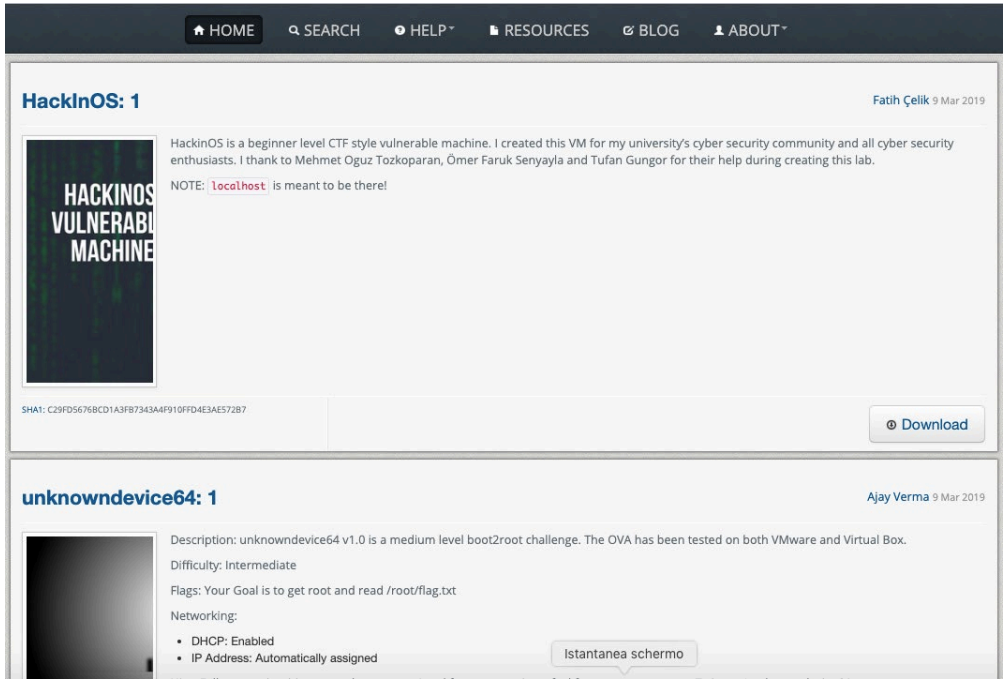
Sistemi Operativi Utilizzati

- L'ambiente operativo del corso sarà costituito dalle seguenti componenti principali
  - Kali Linux (ed eventualmente Parrot, BackBox, etc)
  - Metasploitable 1 (MS1)
  - Metasploitable 2 (MS2)
  - Metasploitable 3 (MS3)
  - Windows XP
  - …

Ambiente Operativo

Ulteriori Sistemi Operativi

- Eventuali altri sistemi operativi vulnerabili «by design» possono essere ottenuti da VulnHub o da fonti simili
  - https://www.vulnhub.com/

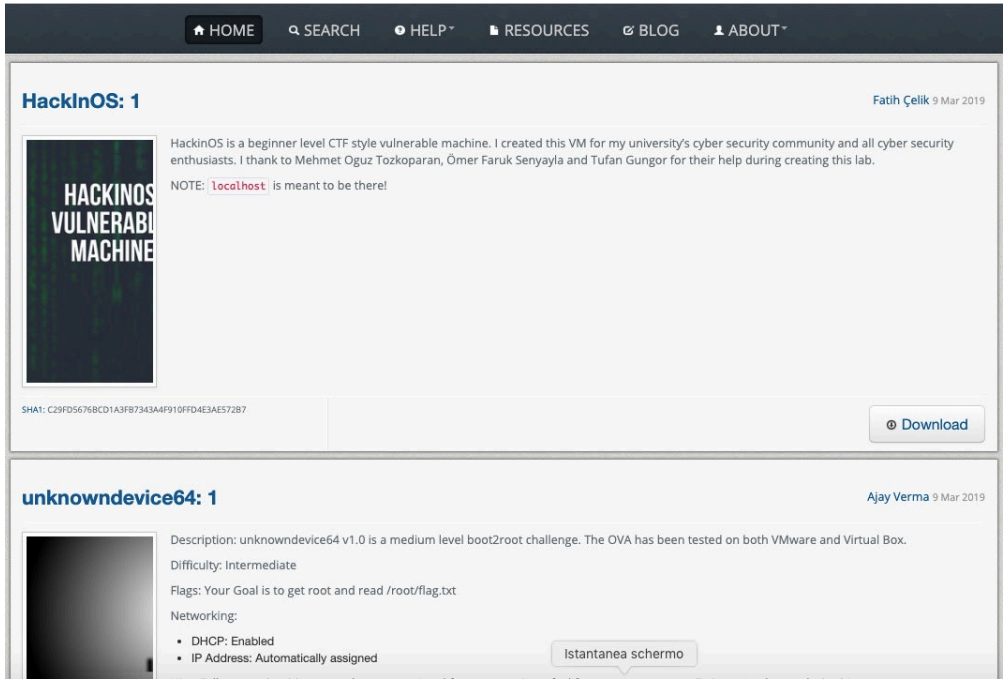


Ambiente Operativo

Ulteriori Sistemi Operativi

- Eventuali altri sistemi operativi vulnerabili «by design» possono essere ottenuti da VulnHub o da fonti simili
  - https://www.vulnhub.com/

Fonte utile anche per la scelta delle attività progettuali



Outline

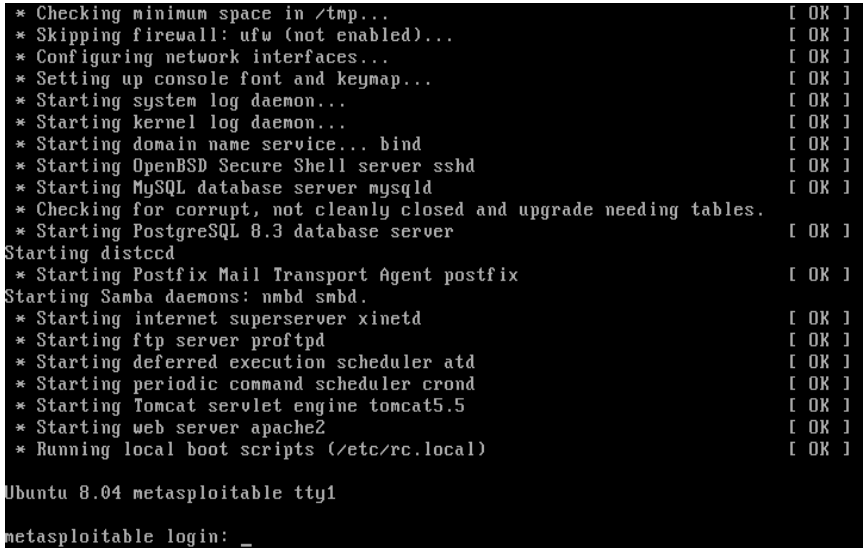
- Ambiente Operativo
- **Asset Vulnerabili**
- Architettura di Rete

Asset Vulnerabili

Metasploitable 1 (MS1)

- Rilasciata il 19 maggio 2010
- Basata su Ubuntu 8.04 Server
- Include numerose vulnerabilità
- https://www.dropbox.com/s/2pccqfcy9eq8ajg/Metasploitable1.ova?dl=0

Username: msfadmin
Password: msfadmin

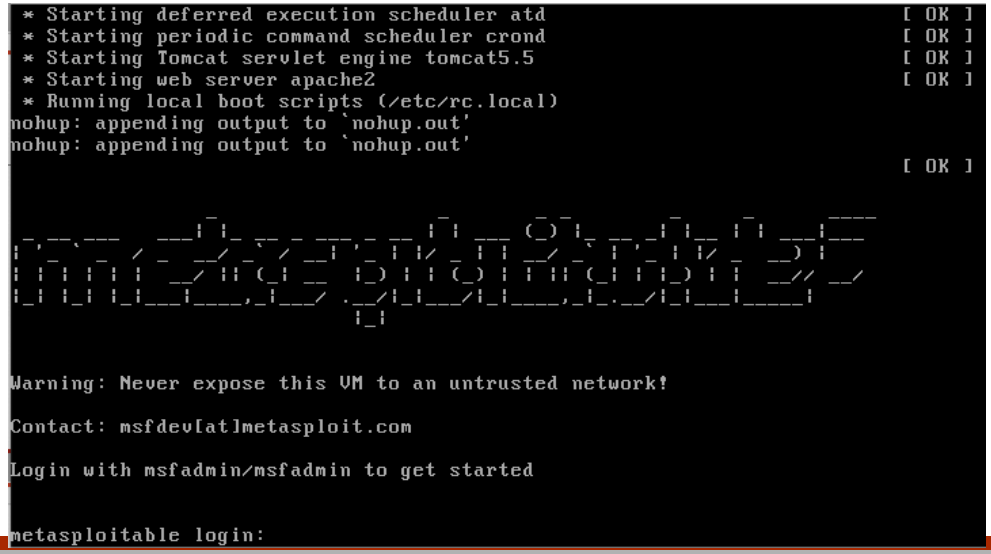


Asset Vulnerabili

Metasploitable 2 (MS2)

- Rilasciata da Rapid7 il 12 (o 13) giugno 2012
- Basata su Ubuntu
- Include numerose vulnerabilità
- https://www.dropbox.com/s/bo3api8egevxxt8/Metasploitable2.ova?dl=0

Username: msfadmin
Password: msfadmin



Asset Vulnerabili

Metasploitable 3 (MS3)

- Framework che permette di creare VM vulnerabili «by design»
  - Tipicamente basate su Windows 2008 Server
  - Ma anche su altre versioni di Windows e Linux (ad es., Ubuntu)

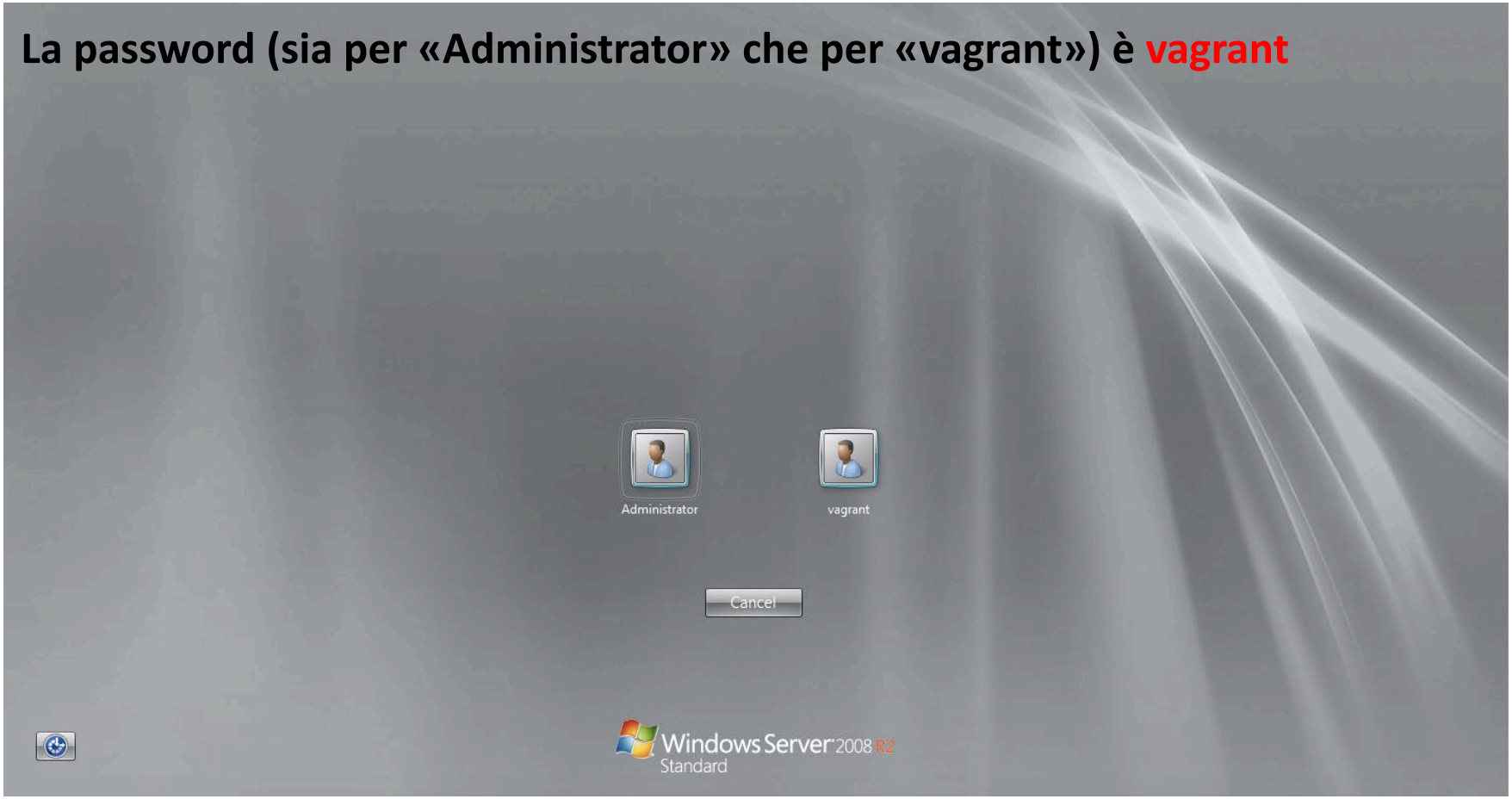
- Rilasciata da Rapid7 il 15 novembre 2016

- https://www.dropbox.com/s/vhn9i41i2r51axe/metasploitable3.ova?dl=0

Asset Vulnerabili

Metasploitable 3 (MS3)

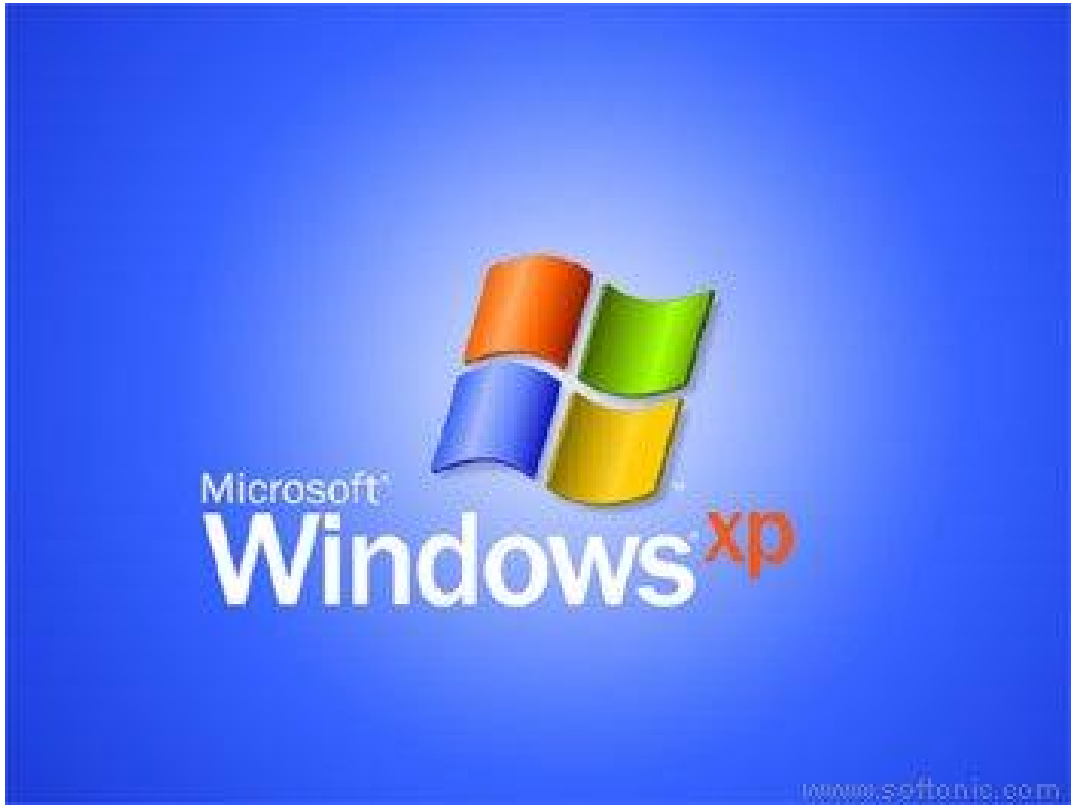
La password (sia per «Administrator» che per «vagrant») è vagrant



Asset Vulnerabili

Microsoft Windows XP SP3

- https://www.dropbox.com/s/g768oa5wchjsmw5/Windows%20XP%2064%20Bit%20ENG.ova?dl=0



Outline

- Ambiente Operativo
- Asset Vulnerabili
- **Architettura di Rete**

Architettura di Rete

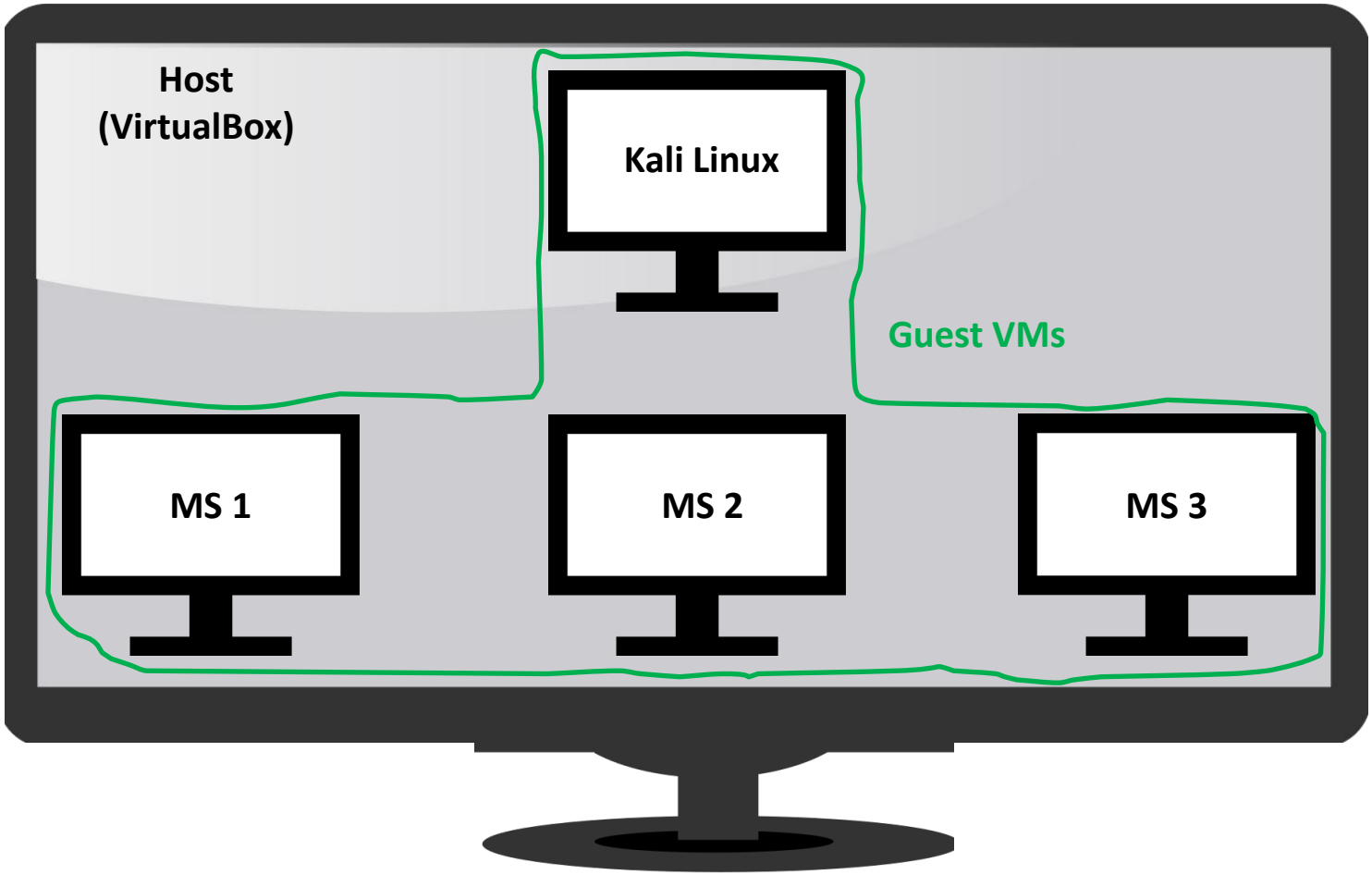
Requisiti

- Tutte le macchine virtuali devono poter
  - Comunicare tra loro
  - Accedere alla rete Internet

- Le macchine presenti sulla rete Internet non devono poter accedere alle macchine virtuali

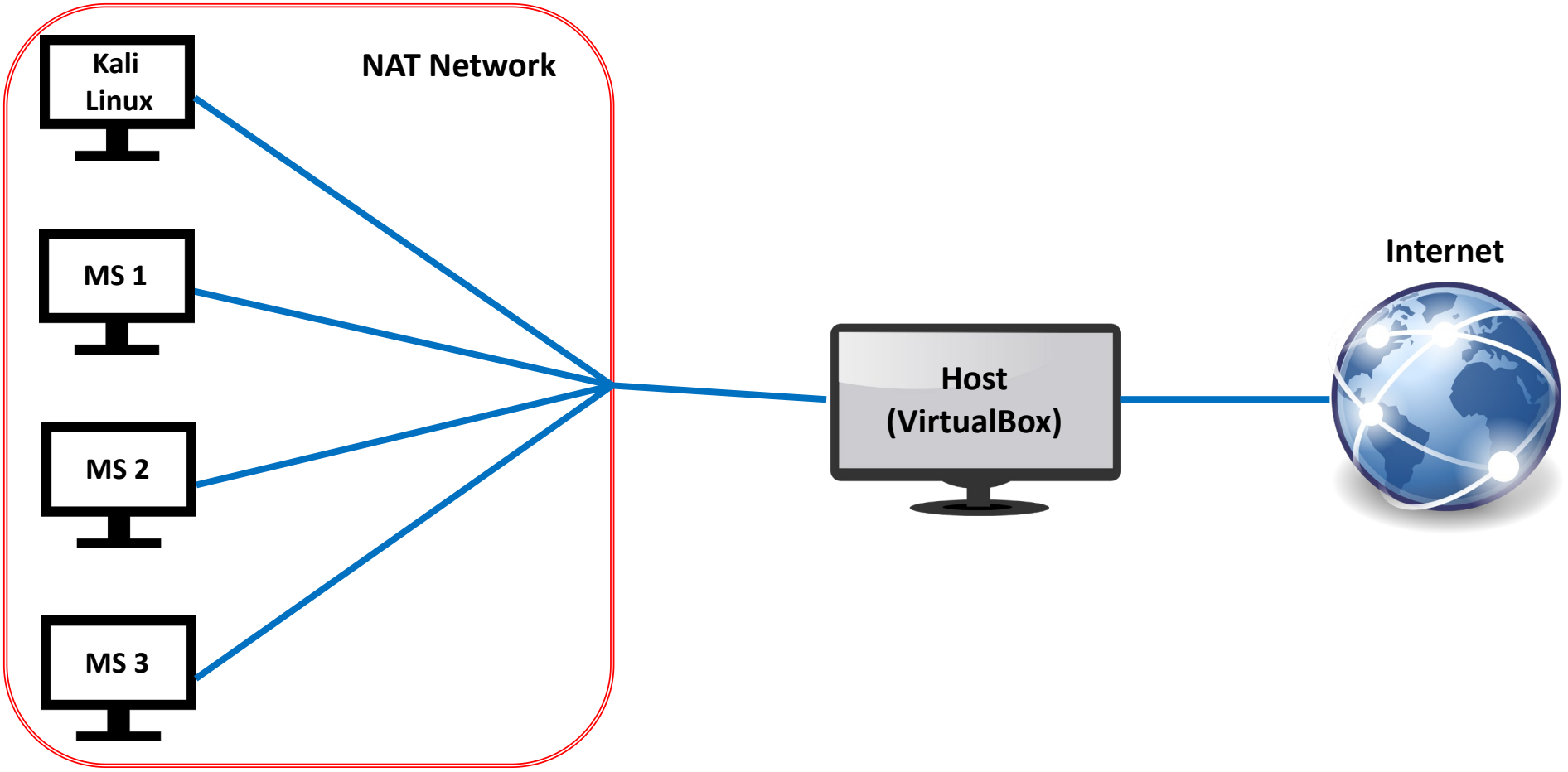
Architettura di Rete

Overview



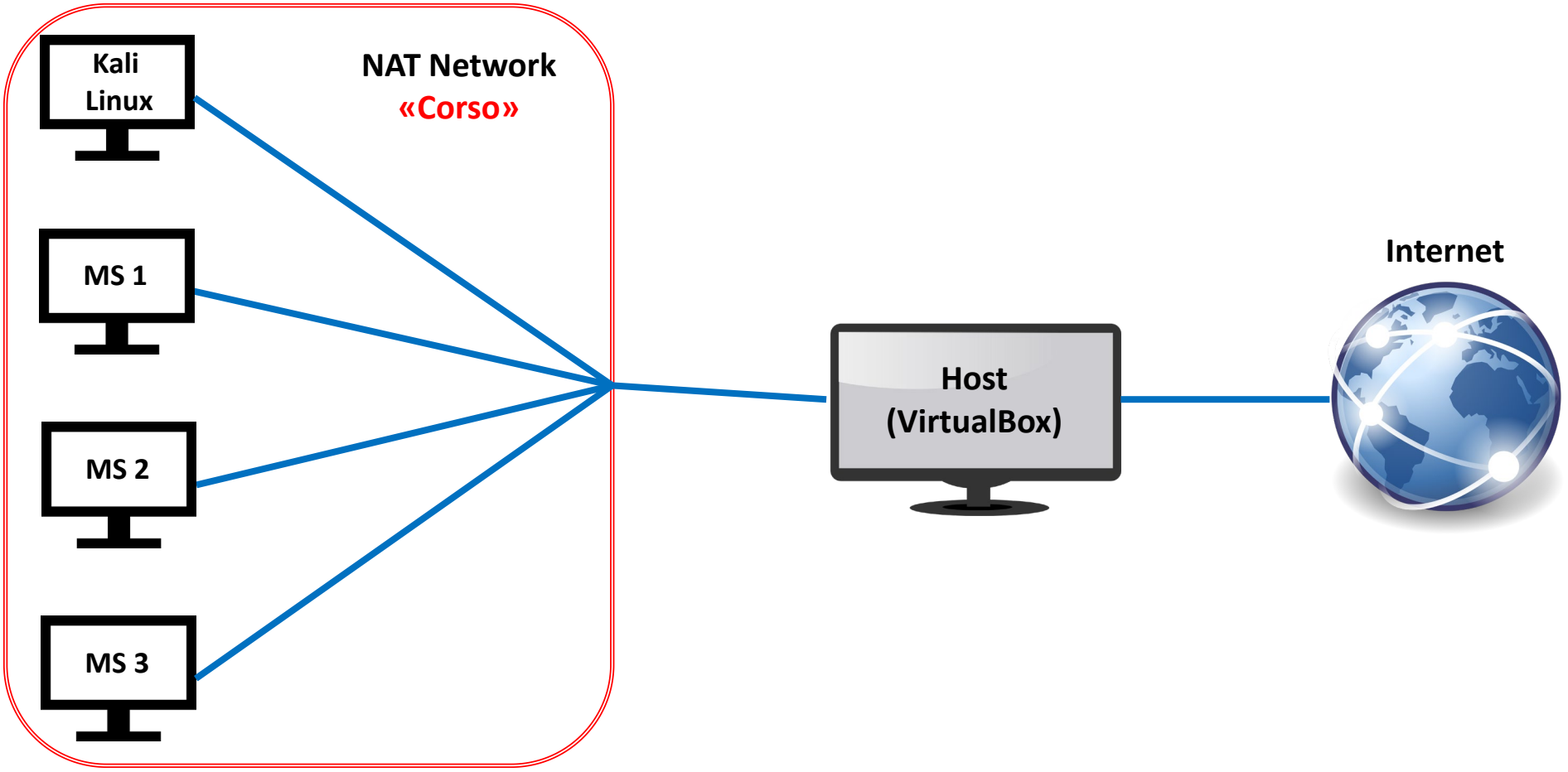
Architettura di Rete

Overview



Architettura di Rete

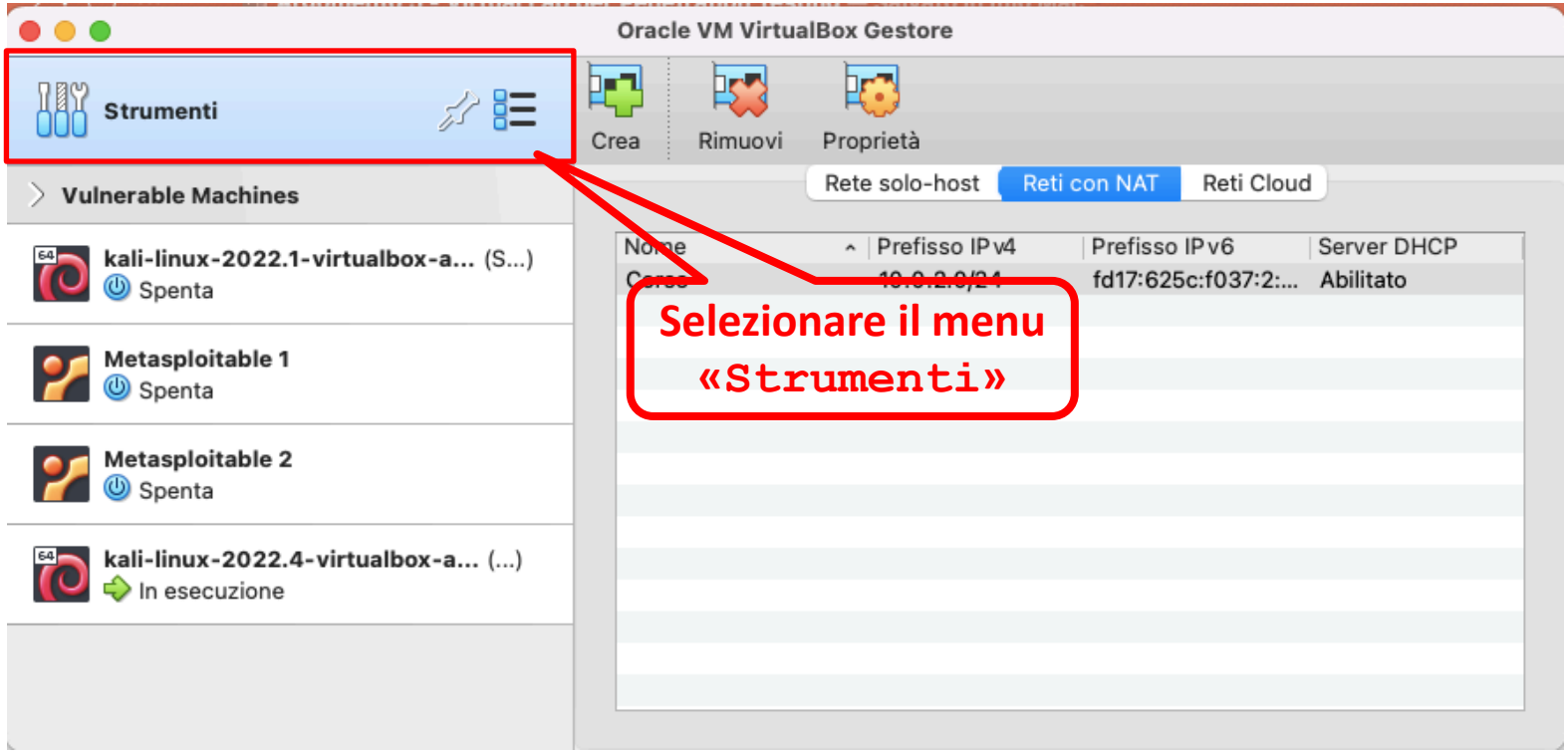
Overview



Architettura di Rete

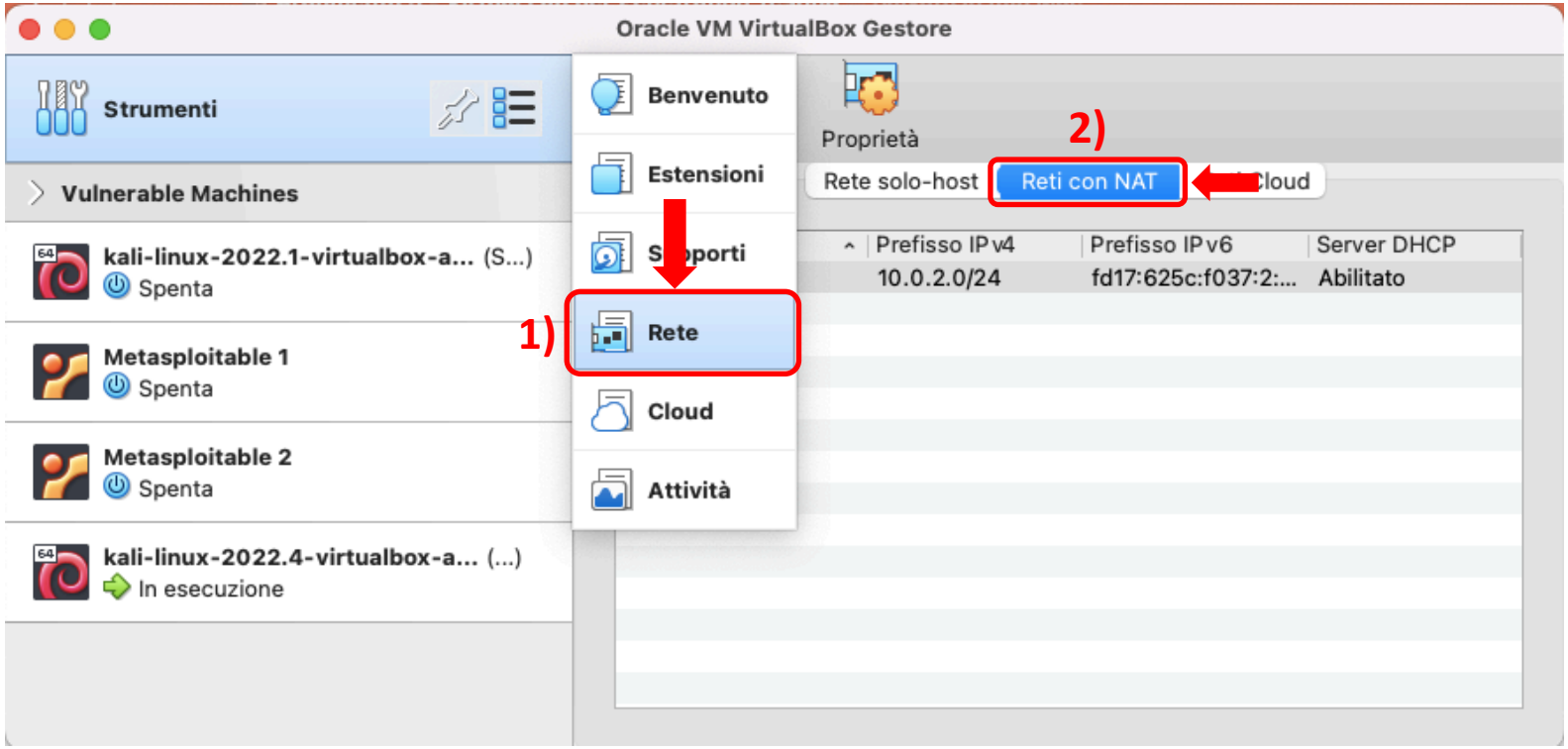
Creazione della rete «Corso» in Virtual Box - macOS

- L'architettura di rete mostrata in precedenza verrà realizzata utilizzando Virtual Box



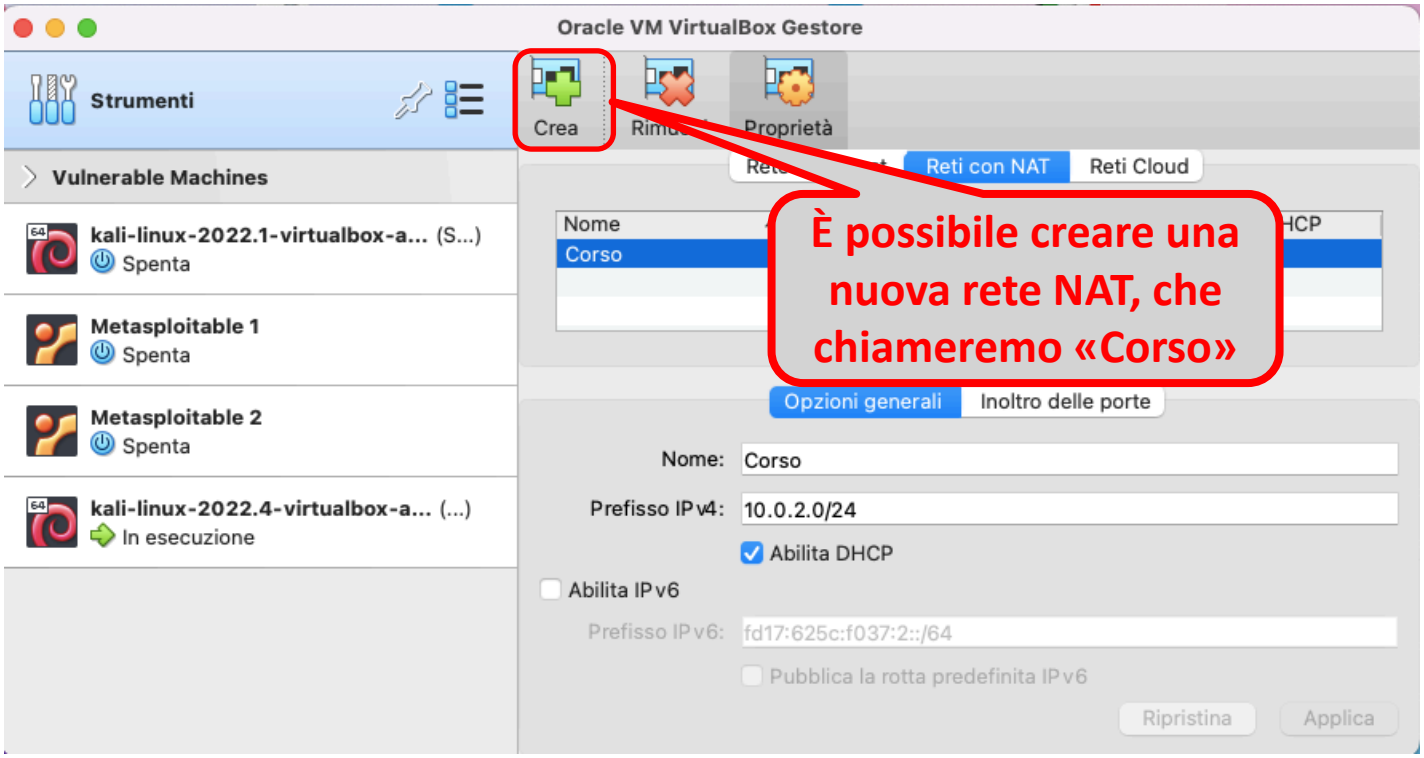
Architettura di Rete

Creazione della rete «Corso» in Virtual Box - macOS



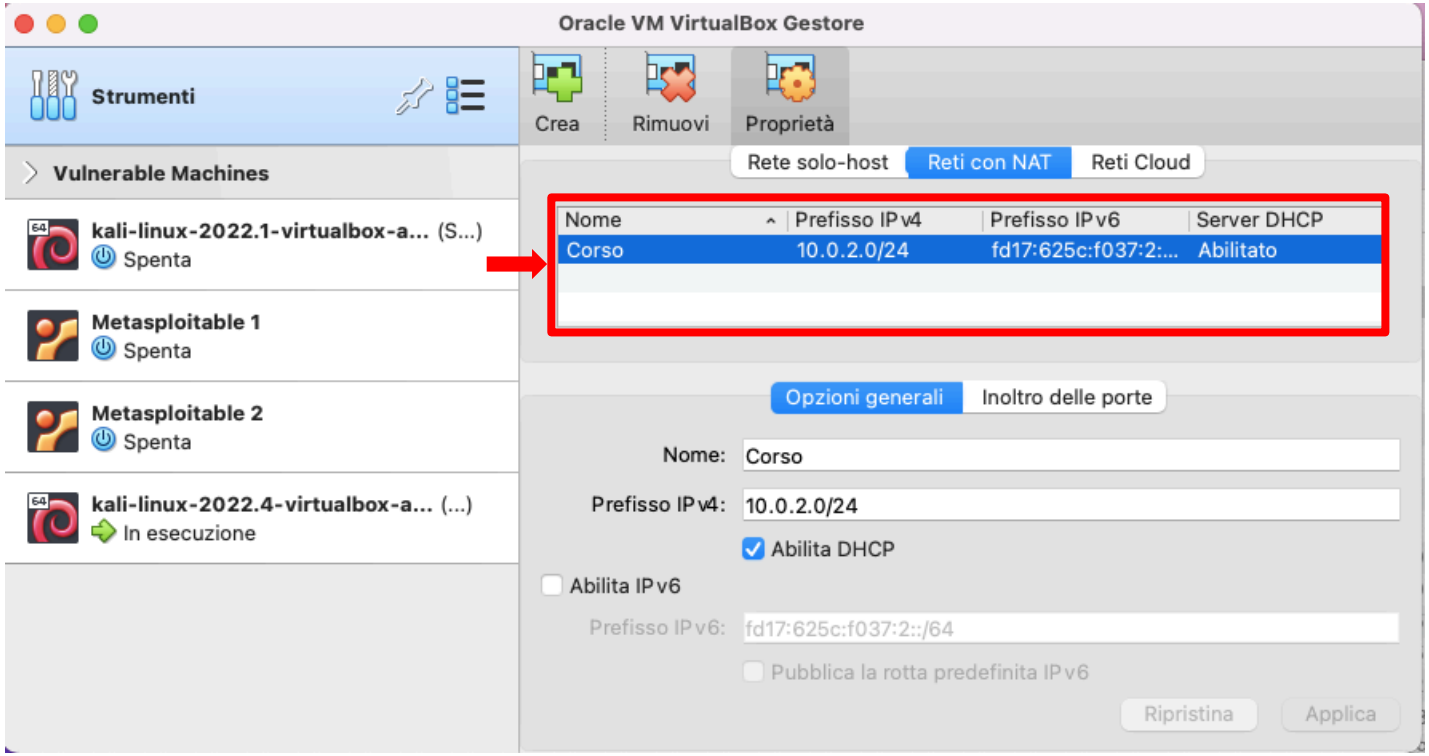
Architettura di Rete

Creazione della rete «Corso» in Virtual Box - macOS



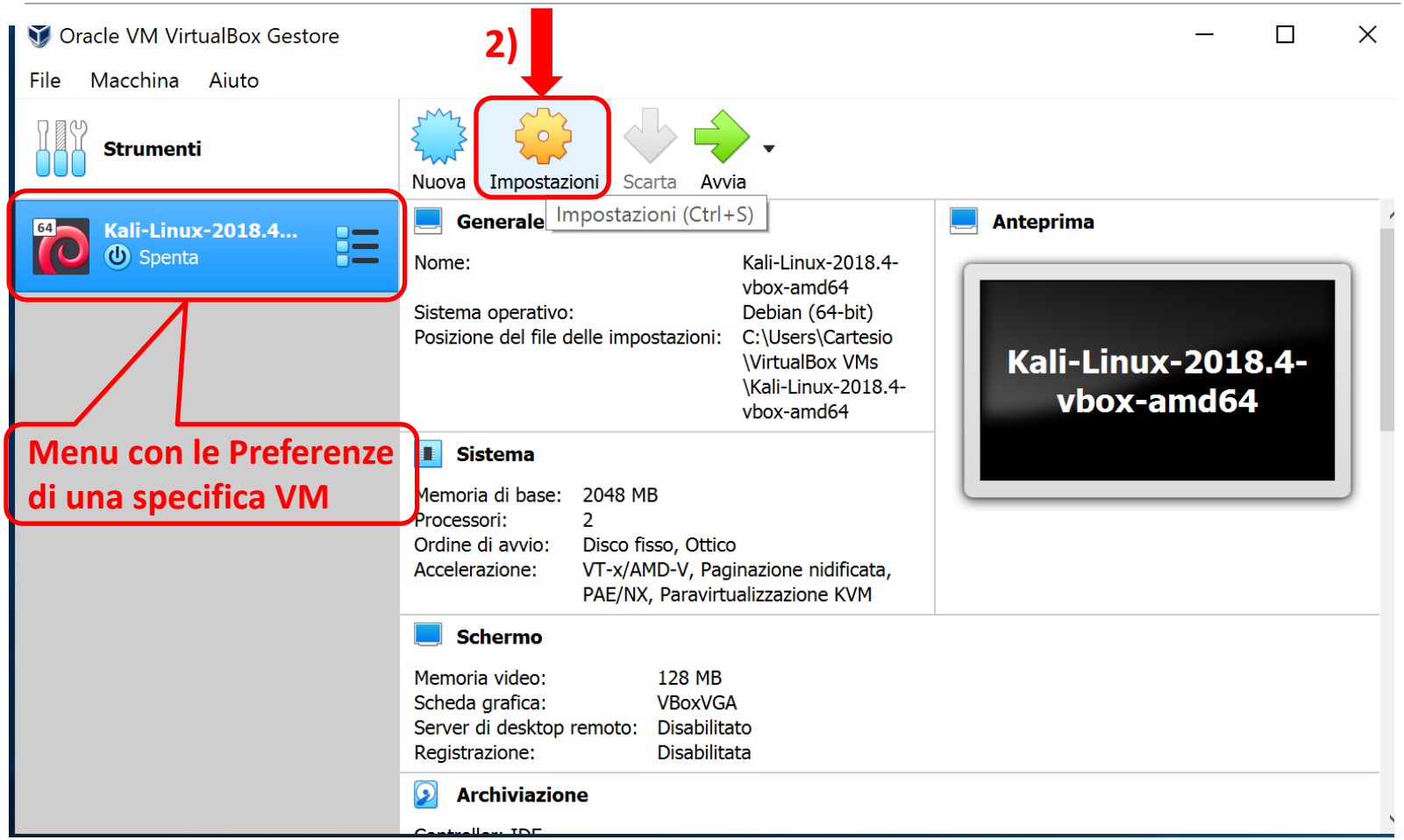
Architettura di Rete

Creazione della rete «Corso» in Virtual Box - macOS



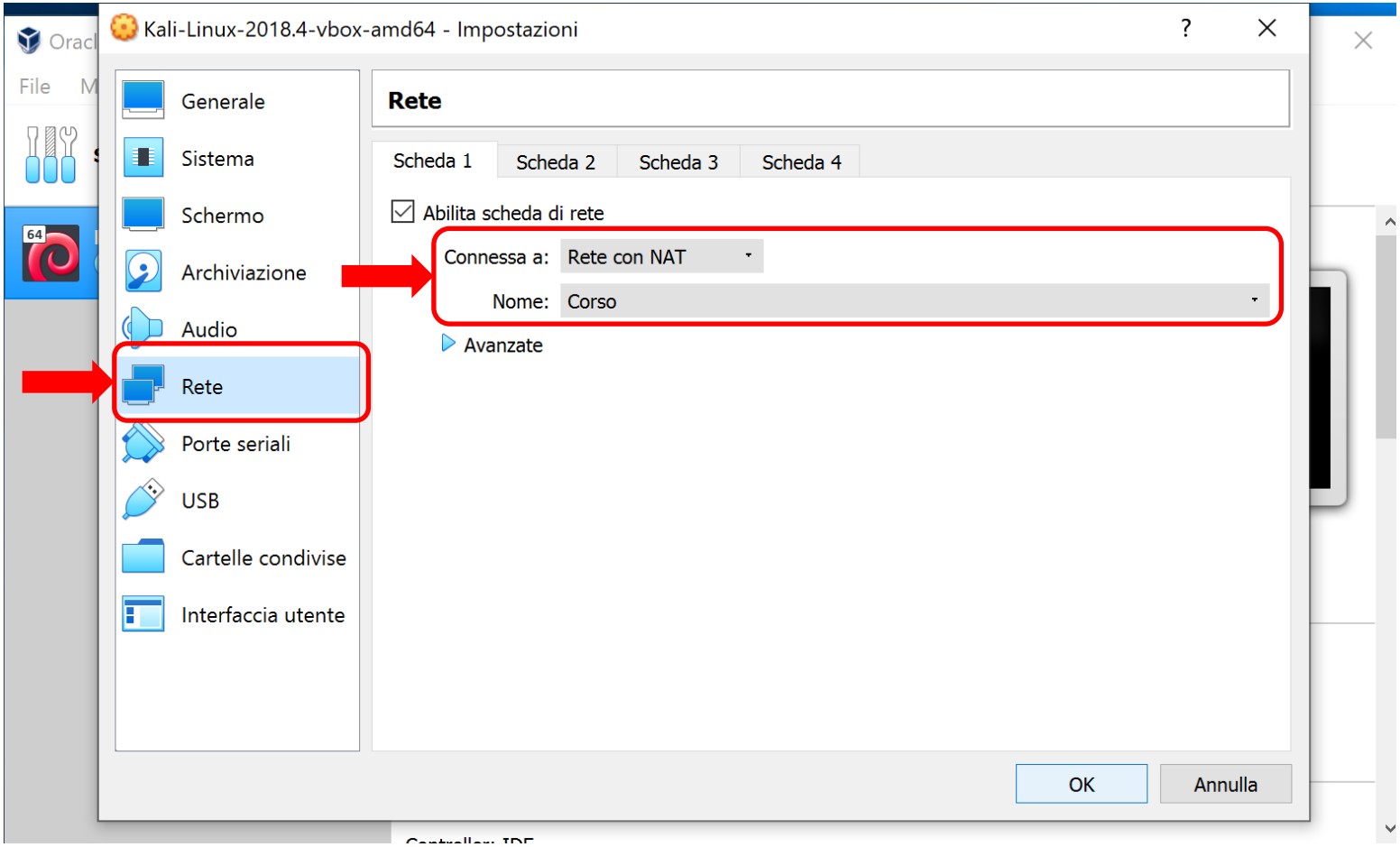
Architettura di Rete

Aggiunta di una VM alla Rete «Corso» – Windows



Architettura di Rete

Aggiunta di una VM alla Rete «Corso» – Windows



Bibliografia

- **Kali Linux 2 - Assuring Security by Penetration Testing. Third Edition**. Gerard Johansen, Lee Allen, Tedi Heriyanto, Shakeel Ali. Packt Publishing. 2016
  - Capitolo 1