

Per questo esercizio ho configurato il laboratorio visuale su Oracle VirtualBox.

Obiettivo: creare un ambiente di test isolato, composto da tre macchine virtuali in grado di comunicare tra loro tramite rete interna, completamente separate dal sistema host e da internet.

Creazione delle macchine virtuali:

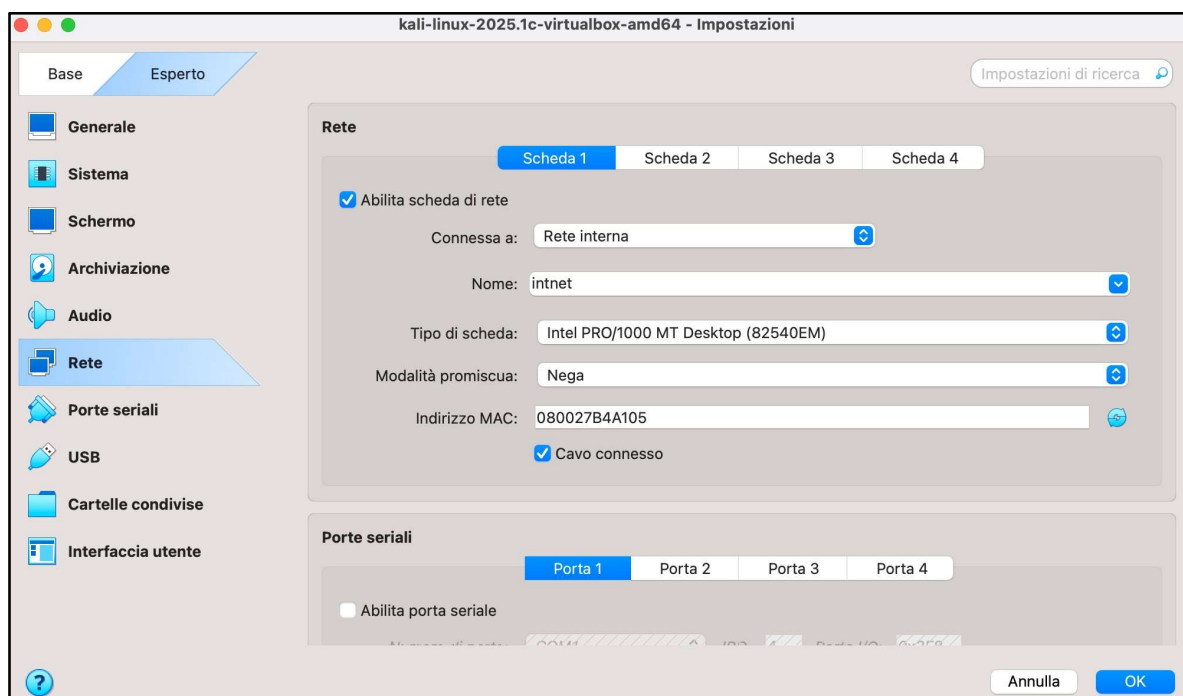
Kali linux, l'ho creata partendo da un'immagine ISO ufficiale e installato il tutto con impostazioni e nome utente e password di default.

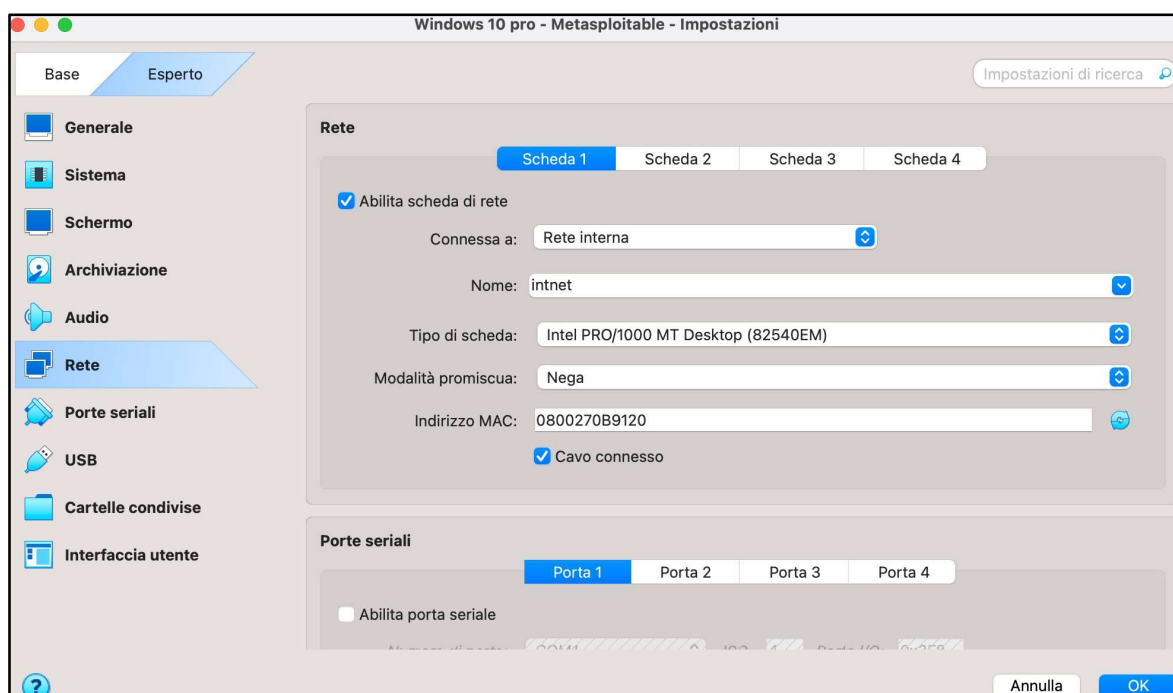
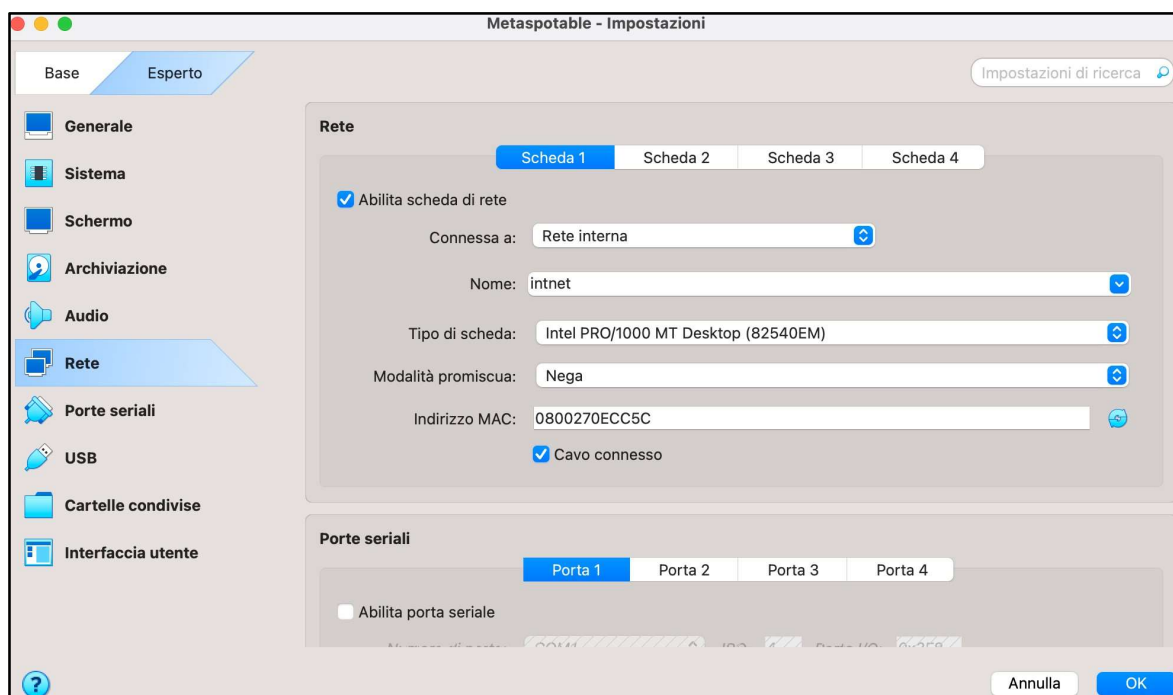
Metaspotable, l'ho creata scaricando l'immagine dal sito ufficiale che fornisce un file .vmdk già pronto. Su virtualbox ho creato una nuova macchina virtuale Linux, specificando di usare il disco virtuale scaricato. Ho avviato il tutto con le credenziali di default msfadmin/msfadmin.

Windows 10 pro, l'ho creata utilizzando il file .ova fornito. L'ho importato direttamente in VirtualBox tramite la funzione importa appliance

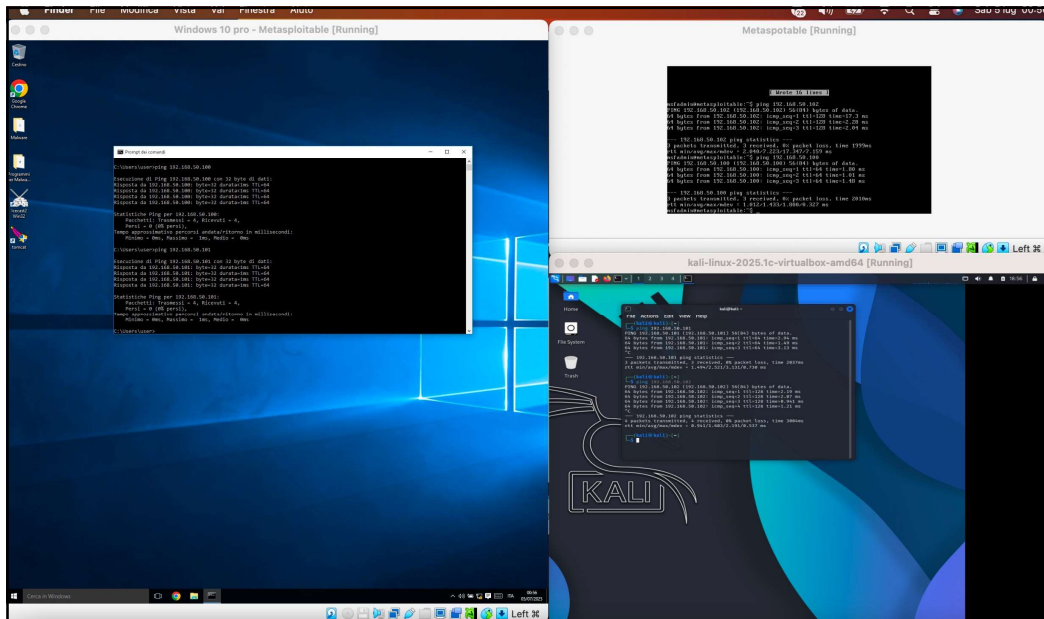
Configurazione della rete

Per permettere alle macchine virtuali di poter comunicare tra loro rimanendo isolato dall'host e da internet, ho impostato la modalità di rete di ciascuna VM su Rete Interna, scegliendo lo stesso nome di rete per tutte ossia intnet



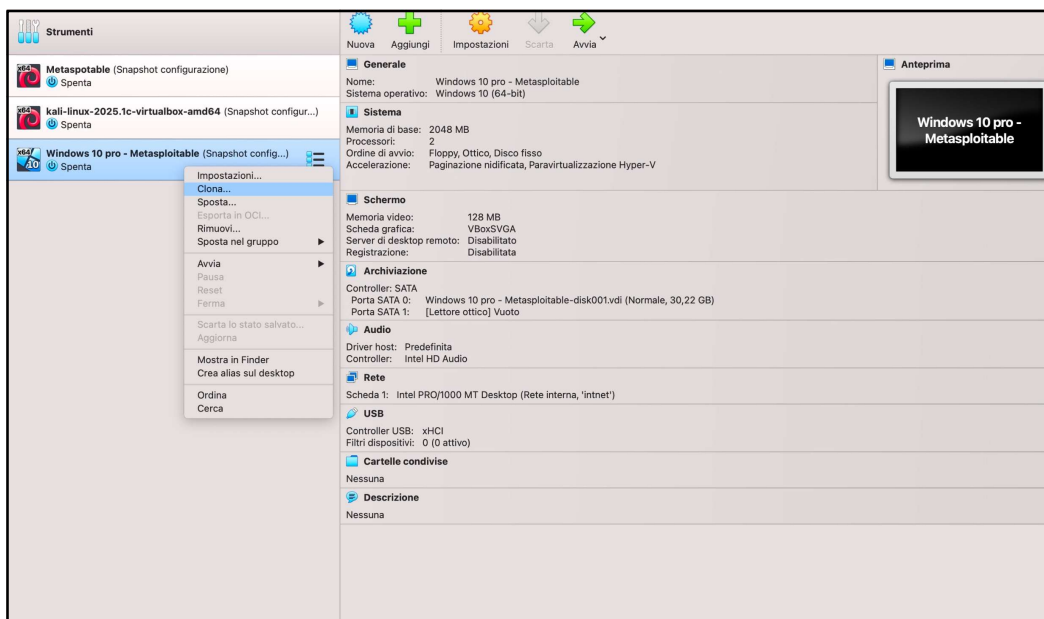


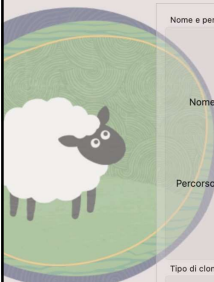
Dopo aver configurato le interfacce di rete delle tre macchine con indirizzi IP statici coerenti (1U2.1G8.50.100, 1U2.1G8.50.101, 1U2.1G8.50.102), ho eseguito alcuni test di connettività tramite il comando ping da ciascuna macchina verso le altre, ottenendo risposta positiva.



Esercizio Facoltativo

Come richiesto nella parte facoltativa dell'esercizio, ho eseguito la clonazione della macchina virtuale Windows 10, creando una copia di recovery chiamata Clone di Windows10 Pro. Ho avviato la copia per verificarne il corretto funzionamento.





Nome e percorso della nuova macchina

Nome: Clone di Windows 10 pro - Metasploitable

Percorso: /Users/miny/VirtualBox VMs

Tipo di clone

☒ Clone completo

☐ Clone collegato

Istantanee

☒ Stato corrente della macchina

☐ Tutto

Opzioni aggiuntive

Criterio indirizzi MAC:

Includi solo gli indirizzi MAC delle schede di rete con NAT

Opzioni aggiuntive:

☐ Mantieni i nomi dei dischi

☐ Mantieni UUID hardware

Strumenti

Metaspotable (Snapshot configurazione)

Spenta

kali-linux-2025.1c-virtualbox-amd64 (Snapshot configur...)

Spenta

Windows 10 pro - Metasploitable (Snapshot config...)

Spenta

Nuova

Aggiungi

Impostazioni

Scarta

Avvia

Generale

Nome: Windows 10 pro - Metasploitable

Sistema operativo: Windows 10 (64-bit)

Sistema

Memoria di base: 2048 MB

Processori: 2

Ordine di avvio: Floppy, Ottico, Disco fisso

Accelerazione: Paginazione nidificata, Paravirtualizzazione Hyper-V

Schermo

Memoria video: 128 MB

Scheda grafica: VBoxSVGA

Server di desktop remoto: Disabilitato

Registrazione: Disabilitata

Archiviazione

Controller: SATA

Porta SATA 0: Windows 10 pro - Metasploitable-disk001.vdi (Normale, 30,22 GB)

Porta SATA 1: [Lettore ottico] Vuoto

Audio

Driver host: Predefinita

Controller: Intel HD Audio

Rete

Scheda 1: Intel PRO/1000 MT Desktop (Rete interna, 'intnet')

USB

Controller USB: xHCI

Filtri dispositivi: 0 (0 attivo)

Cartelle condivise

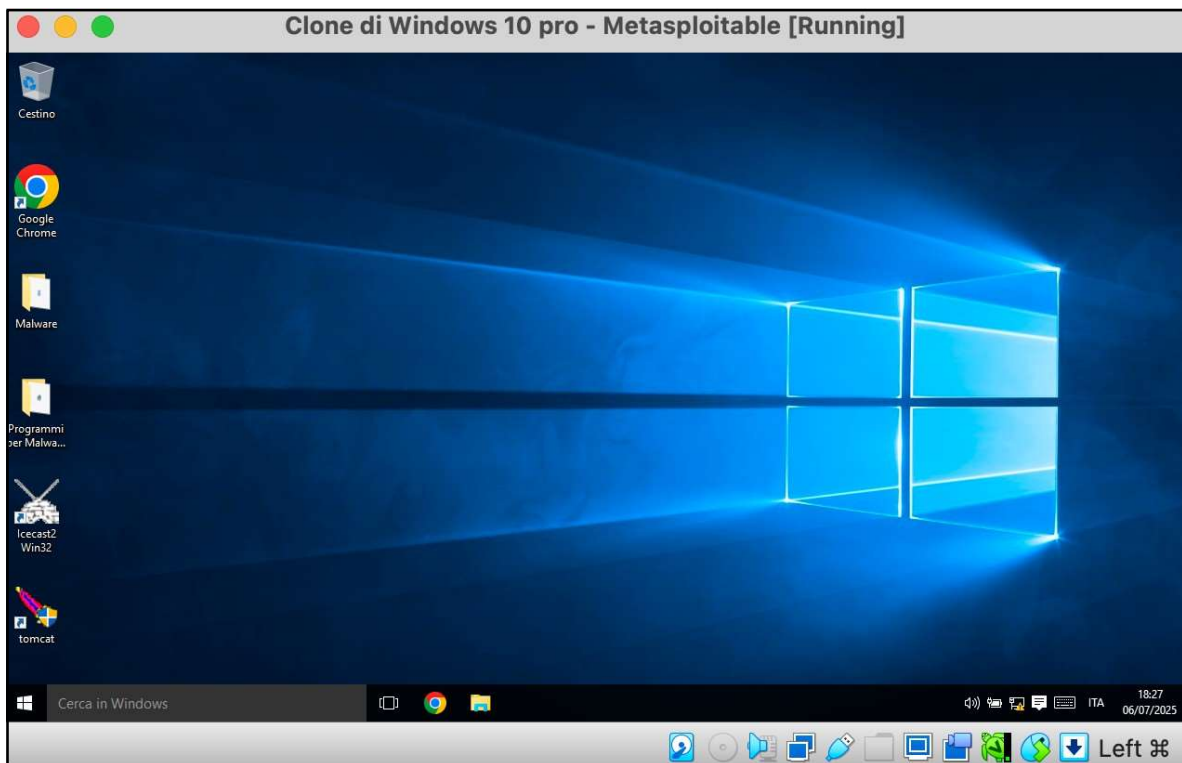
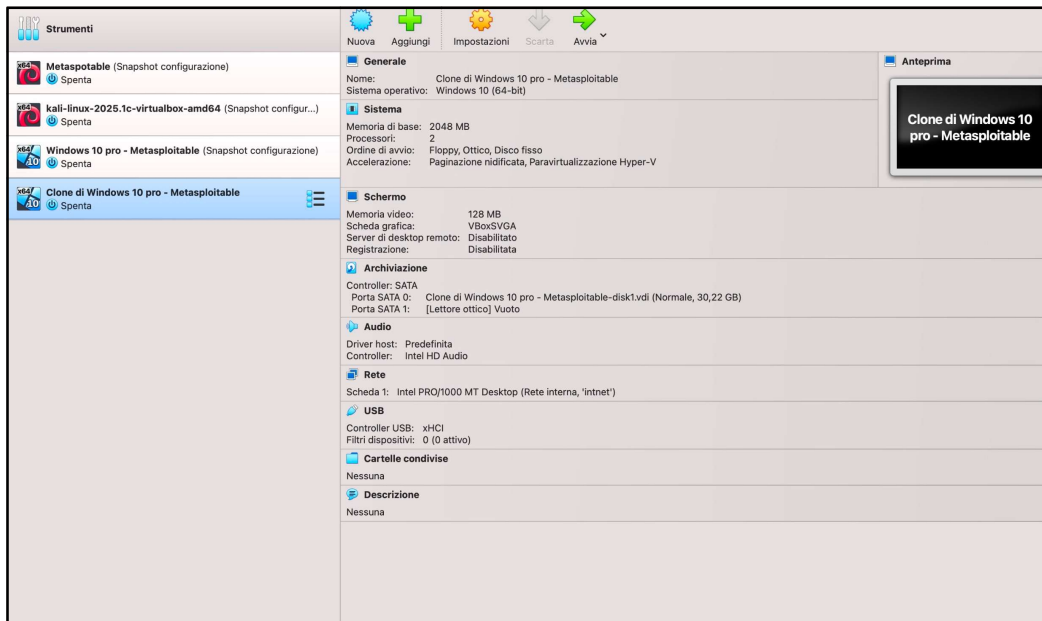
Nessuna

Descrizione

Nessuna

Copia della macchina...

Windows 10 pro - Metasploitable



Considerazioni

Questo laboratorio virtuale rappresenta una base importante per chi lavora o si forma come hacker etico. La possibilità di simulare attacchi e test in un ambiente isolato è fondamentale per sperimentare la sicurezza informatica e l'esperienza pratica.