The Malware Analysis Project 101

> *An Introduction to Malware Analysis*
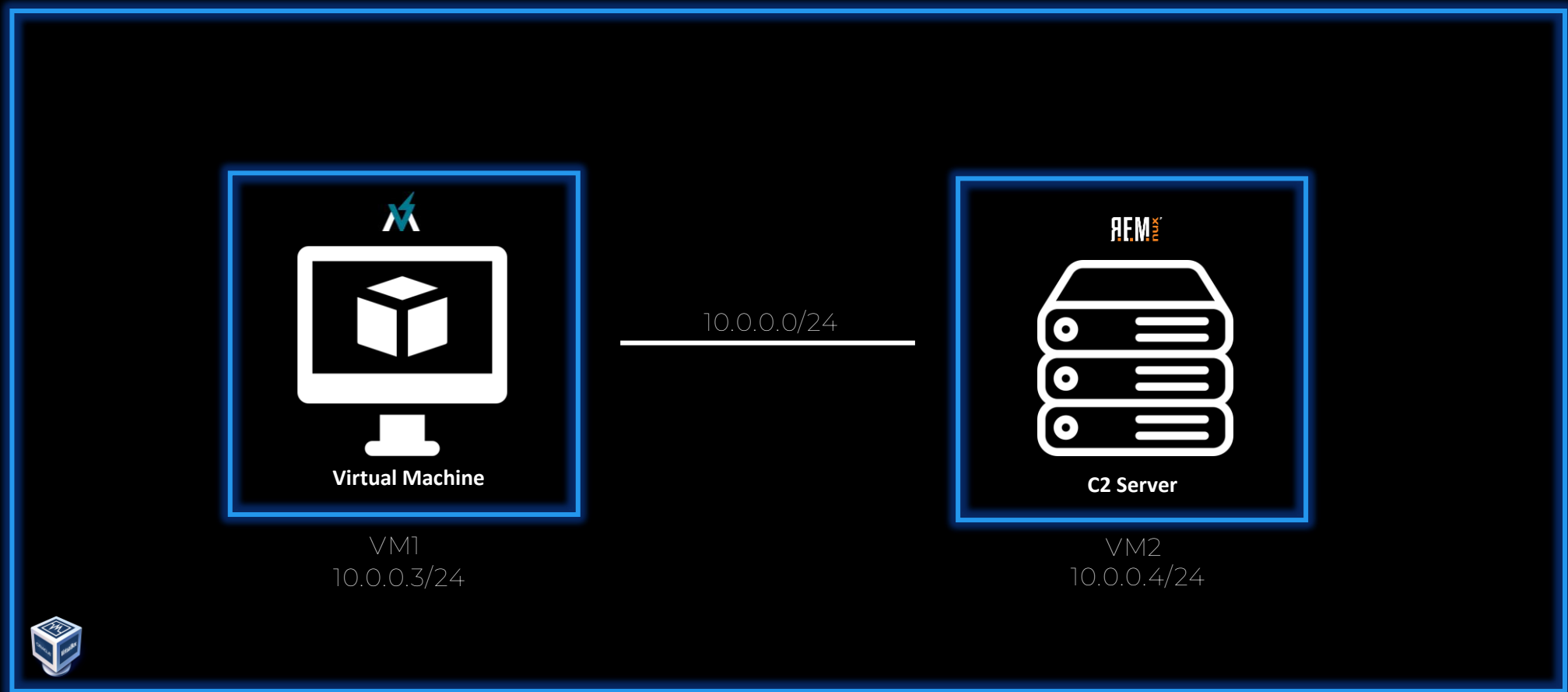
💻 Building an Isolated Analysis Lab

Overview

- Setup an isolated malware analysis environment with malware analysis tools.
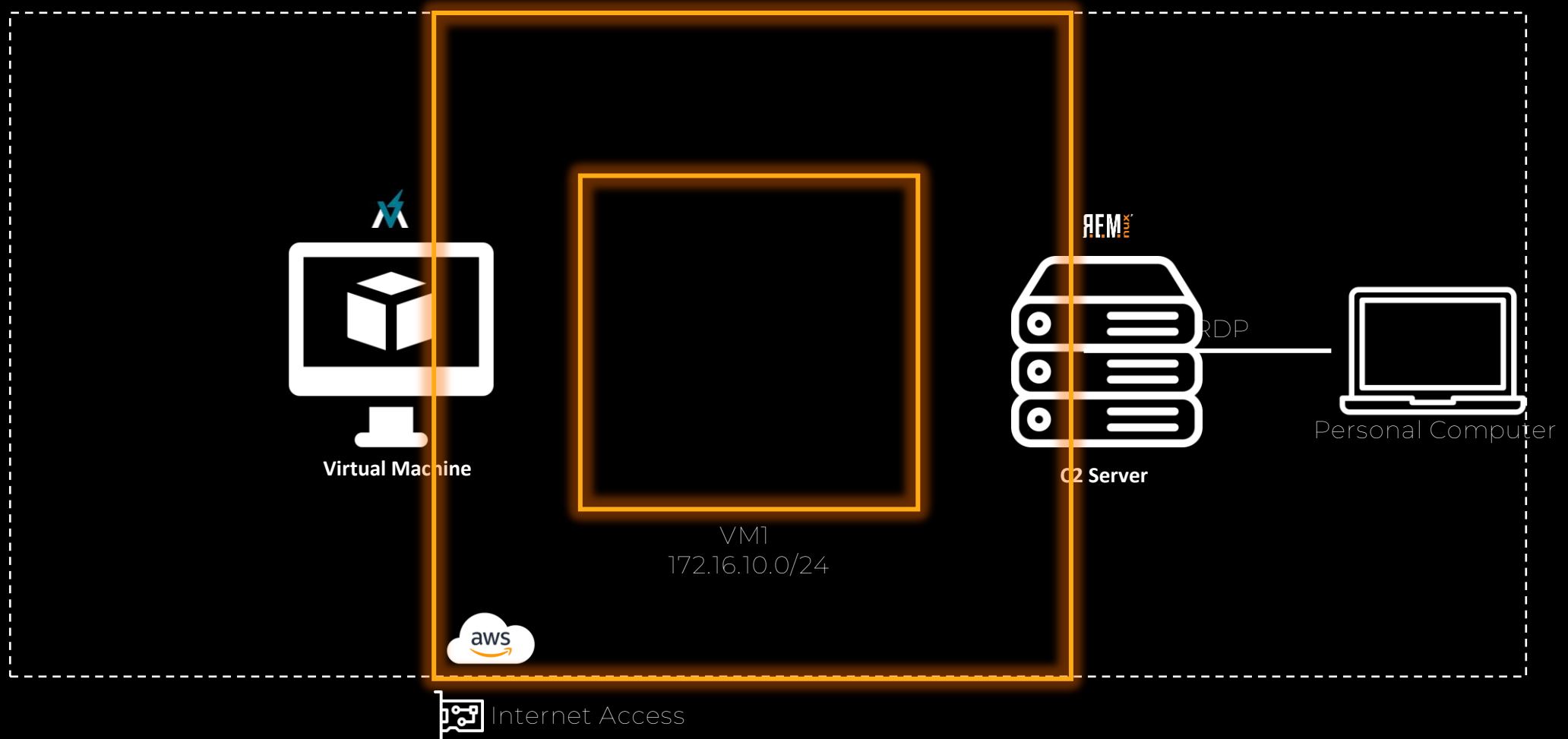- Create an immutable snapshot to restore environment after malware detonation.

Self-hosted

Cloud-hosted

💻 Topology

Virtual Machine

VM1
10.0.0.3/24

10.0.0.0/24

C2 Server

VM2
10.0.0.4/24

Host-only Adapter (no Internet access)

💻 Topology

Virtual Machine

VM1
172.16.10.0/24

C2 Server

RDP

Personal Computer

aws

Internet Access

Credit: https://github.com/adanalvarez/AWS-malware-lab

⊖ Note

- Will require to pause while installation and setup is taking place for:
  - Download VirtualBox
  - Download Windows 10 Enterprise ISO
  - Setup FlareVM
  - Download Remnux
  - Setup EC2 Instance
  - Setup AMI
  - Setup Terraform

- Cloud-Hosted:
  - Will cost money when lab is live (make sure to do `terraform destroy` after completion).
  - If not using Windows as your host, must install an RDP client (macOS: Microsoft Remote Desktop).
  - Must have access to Linux / Unix Terminal. (Windows: Ubuntu 20.04/22.04 WSL).

- Can download slides and notes in the description below.