

**OST**  
Ostschweizer  
Fachhochschule

# Deployment Manager

## Azure Deployment with Hacking-Lab

Ivan Bütler

6. Oktober 2024

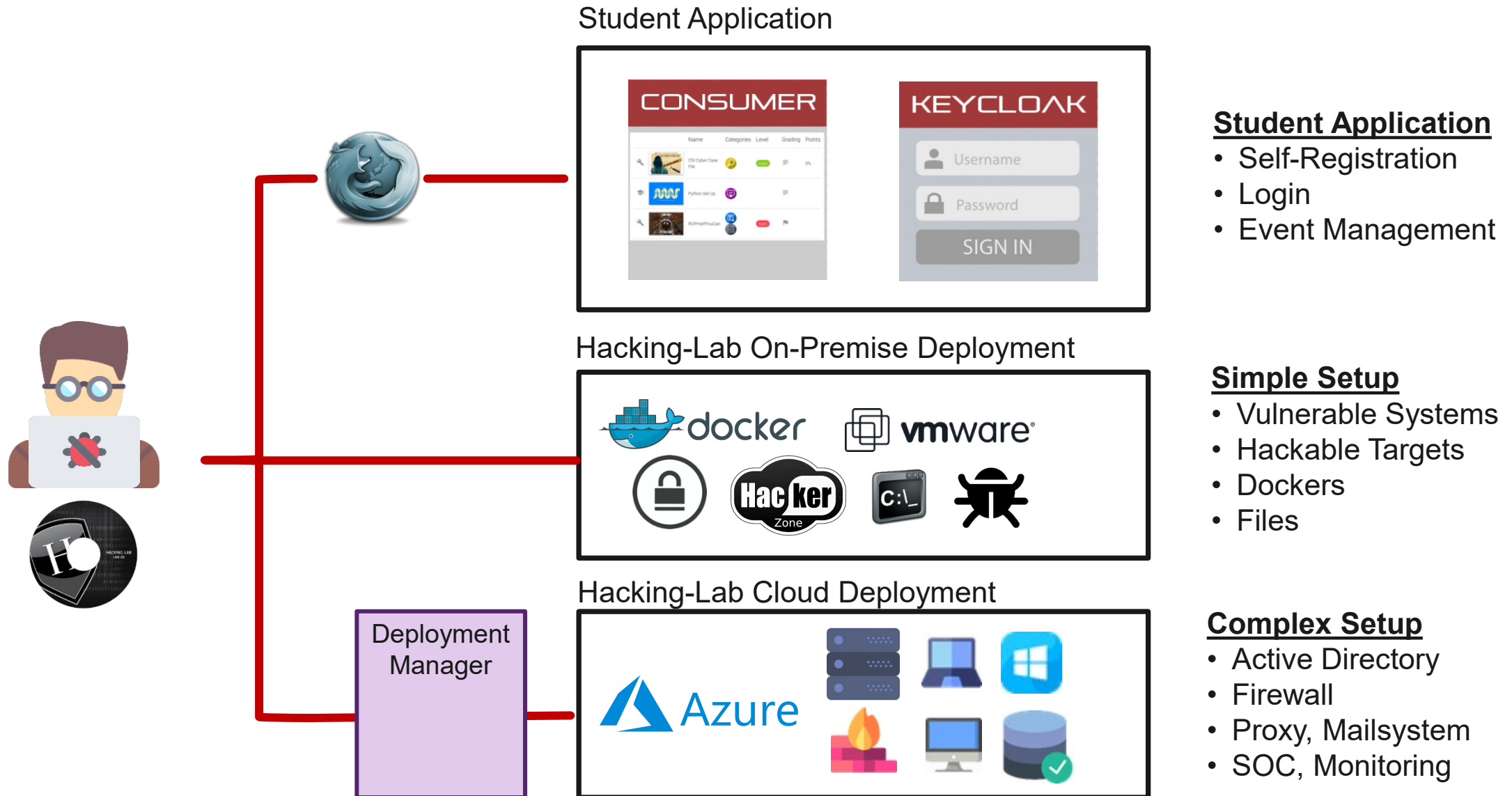
Abteilung Informatik, Rapperswil

## Overview

# Agenda

- Introduction
- Terraform
- Deployment Manager
  - Deploying your Lab
  - Accessing your Lab
  - Destroying your Lab

# Overview Hacking-Lab

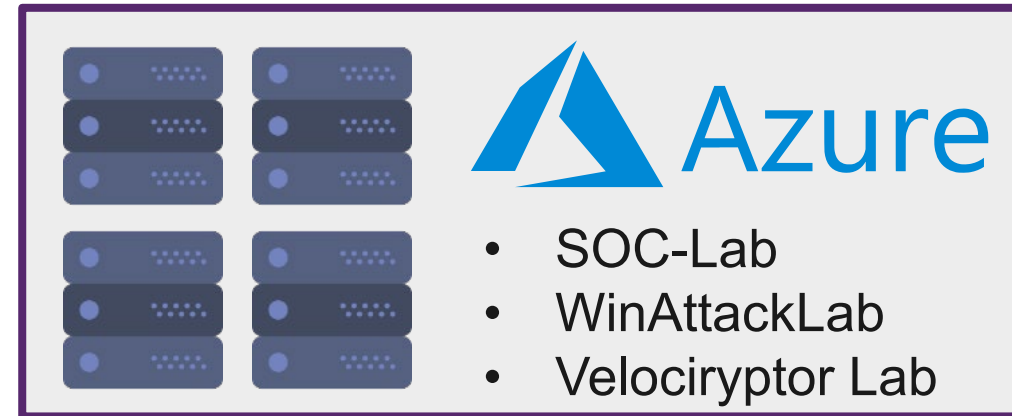


# Deployment Manager

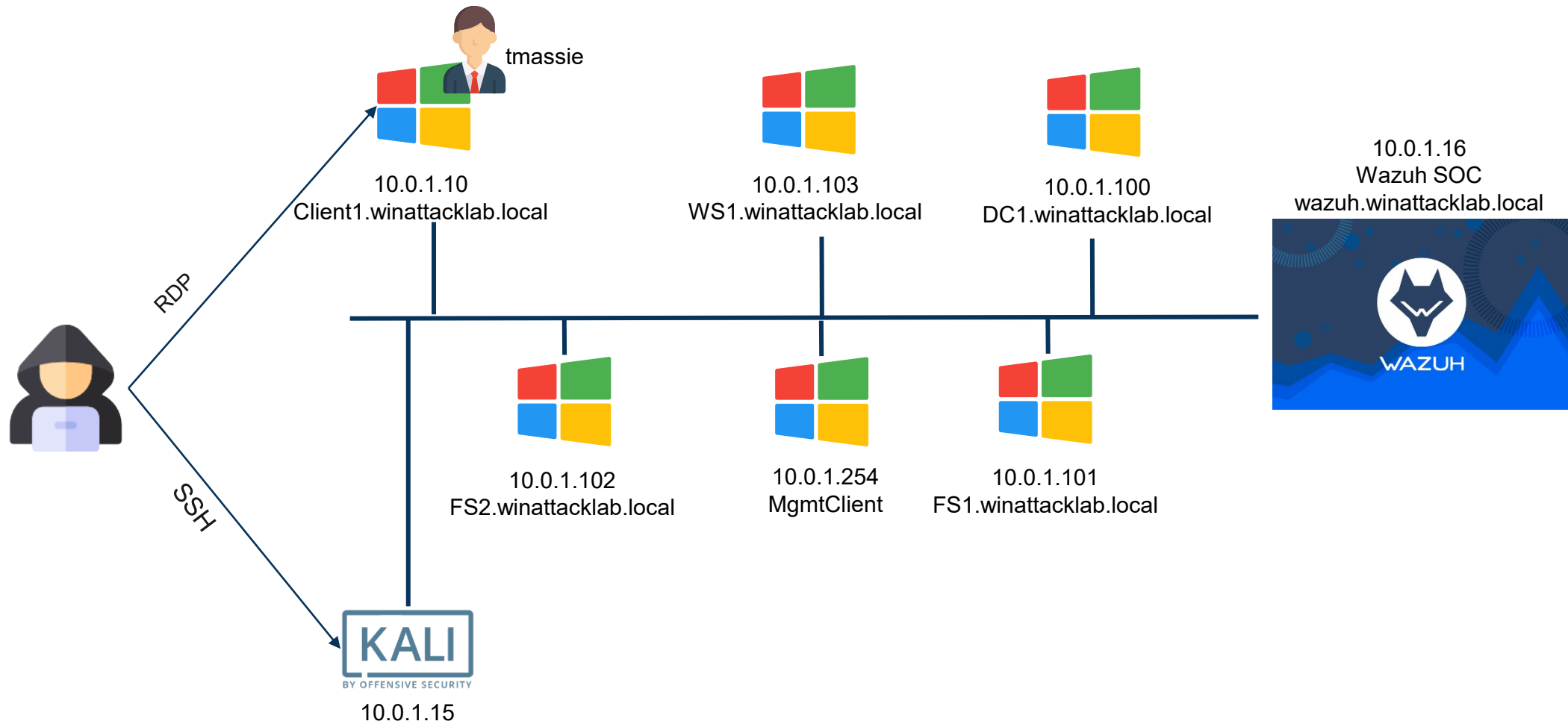
- **WinAttackLab**
  - Vulnerable Active Directory
  - Red-Teaming
- **SOC Lab**
  - Vulnerable Active Directory
  - Monitoring
- **Velociraptor Lab**
  - Vulnerable Active Directory
  - Hunting



Student

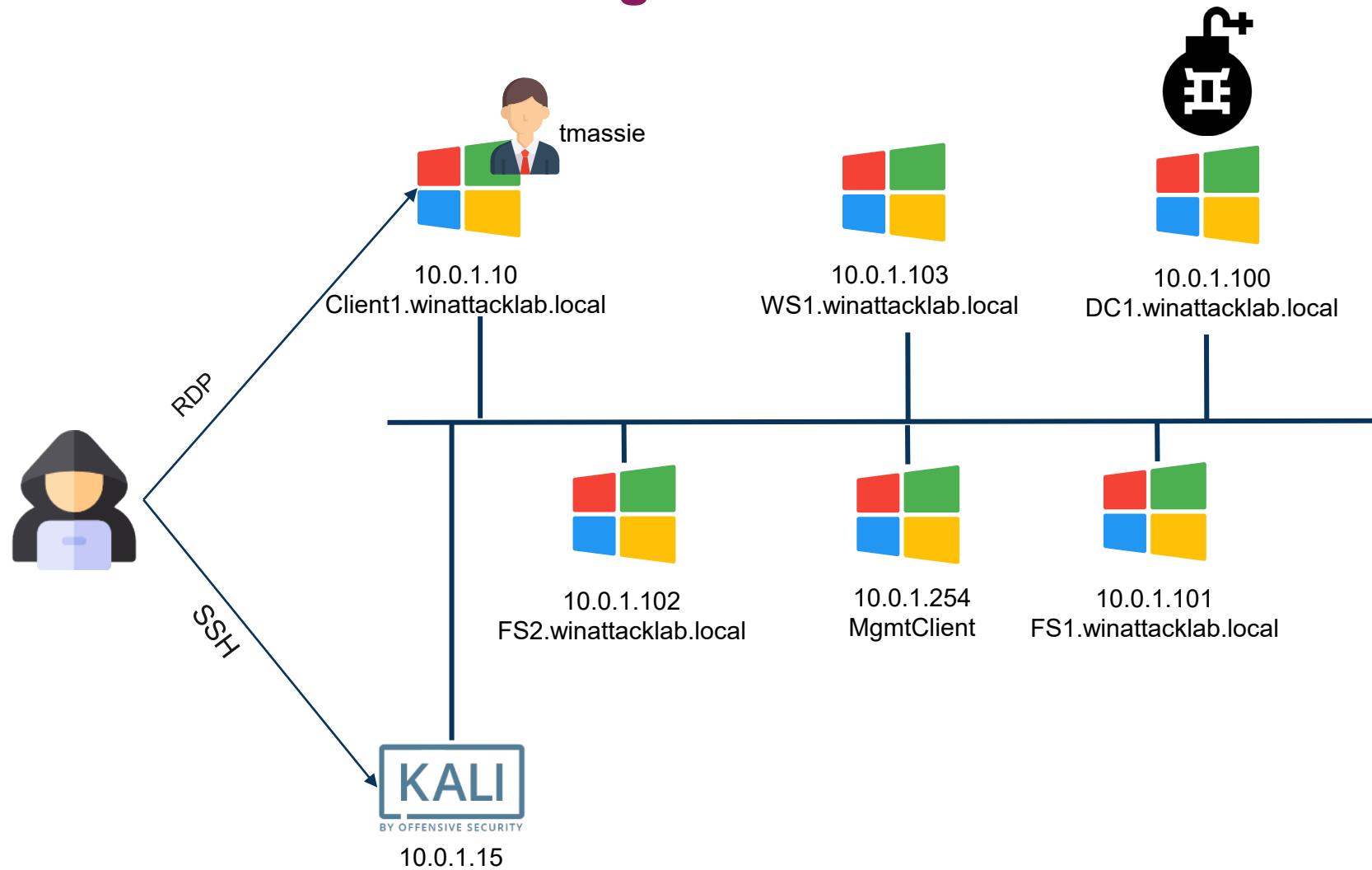


# SOC Lab / Monitoring



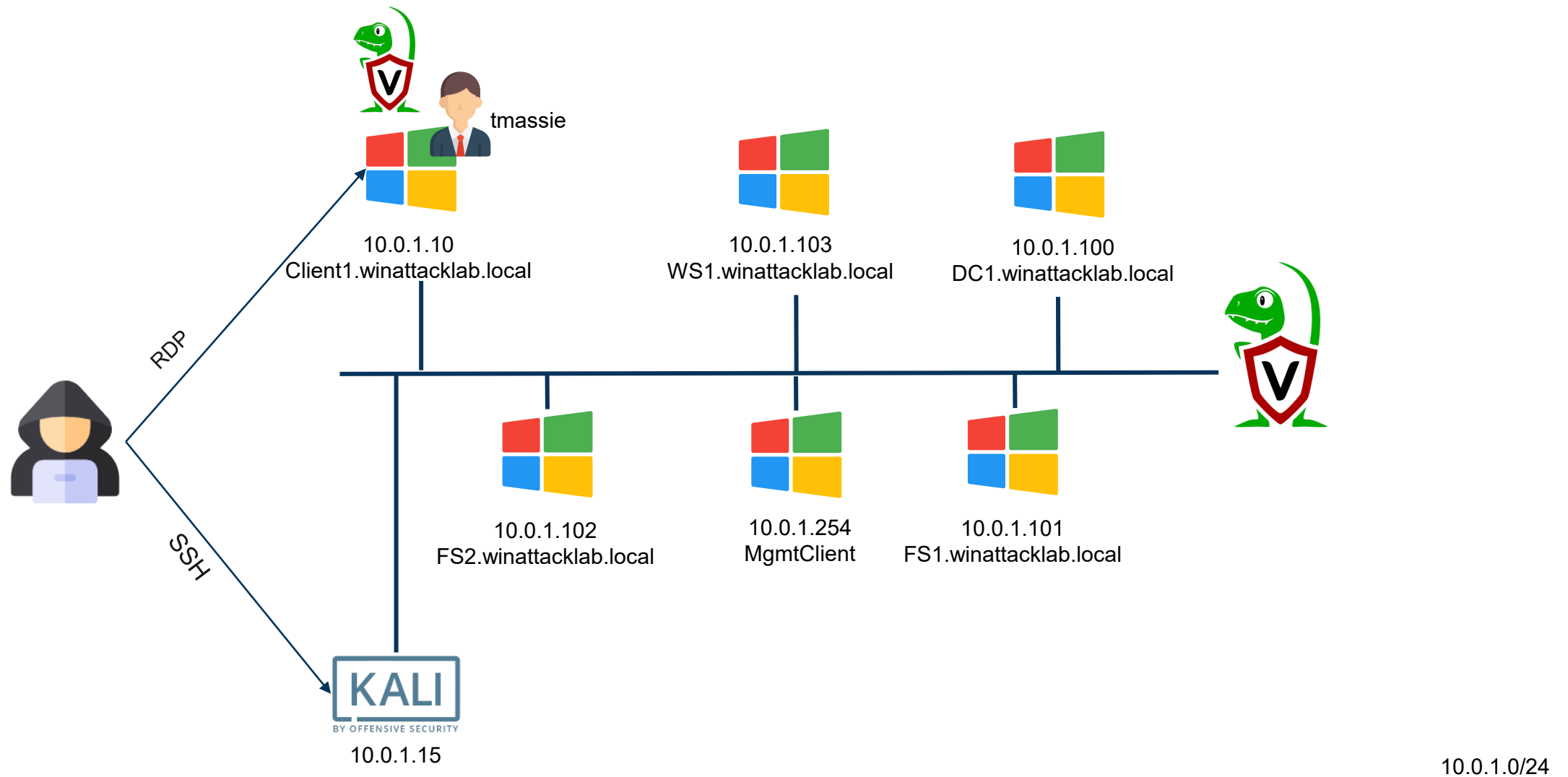


# WinAttackLab / Red-Teaming Lab



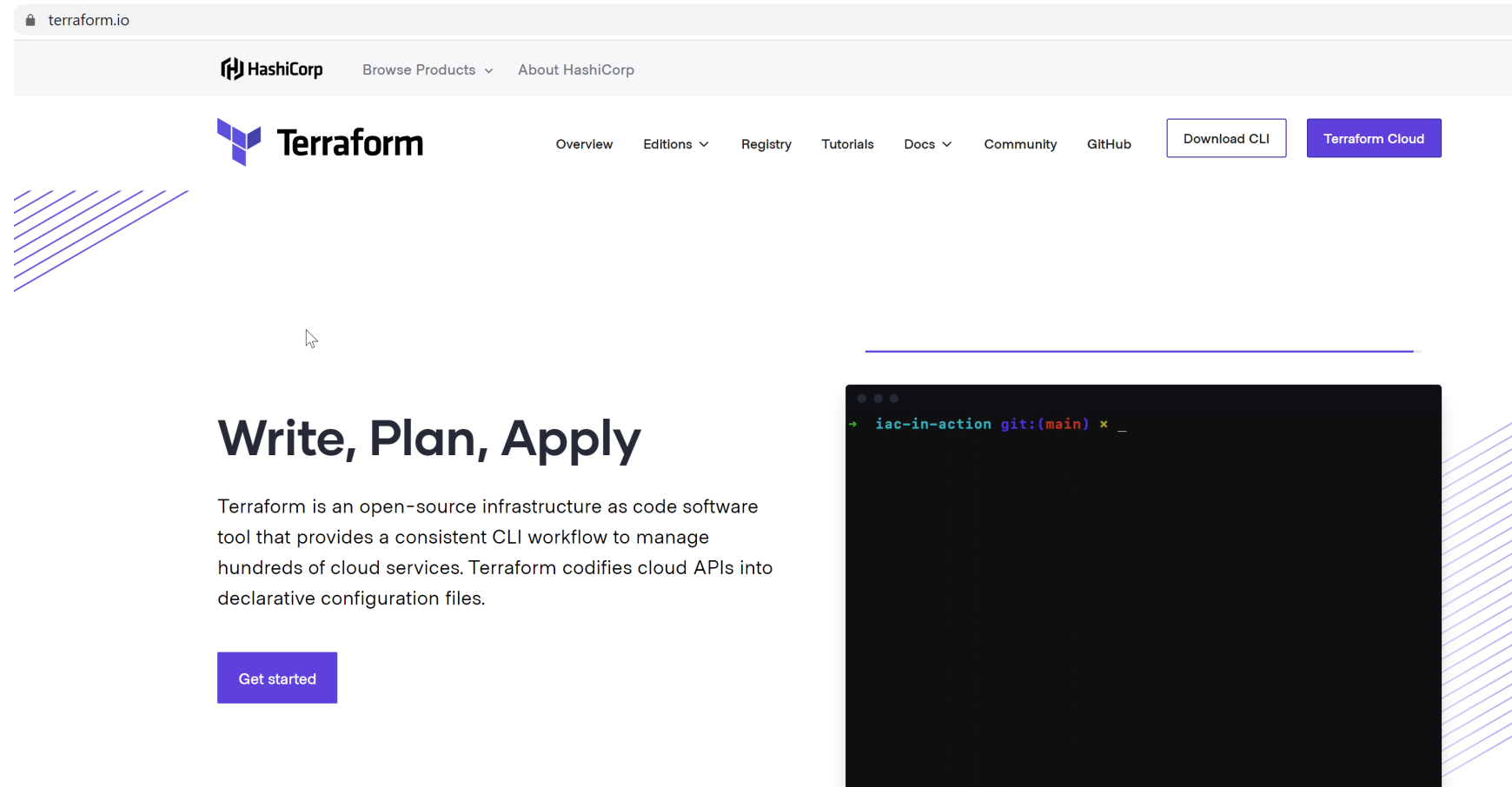
10.0.1.0/24

# Velociraptor Lab / Hunting



# Terraform

# Infrastructure as Code



The screenshot shows the Terraform.io website. At the top, there's a navigation bar with the HashiCorp logo, "Browse Products", and "About HashiCorp". Below this is the Terraform logo and a navigation menu with links: Overview, Editions, Registry, Tutorials, Docs, Community, GitHub, Download CLI, and Terraform Cloud. The main content area features the heading "Write, Plan, Apply" and a paragraph describing Terraform as an open-source infrastructure as code software tool. A "Get started" button is present. To the right, there's a terminal window showing a command: `iac-in-action git:(main) x _`. Decorative blue diagonal lines are on the left and right sides of the main content area.

terraform.io

HashiCorp Browse Products About HashiCorp

**Terraform** Overview Editions Registry Tutorials Docs Community GitHub Download CLI Terraform Cloud

## Write, Plan, Apply

Terraform is an open-source infrastructure as code software tool that provides a consistent CLI workflow to manage hundreds of cloud services. Terraform codifies cloud APIs into declarative configuration files.

Get started

```
iac-in-action git:(main) x _
```



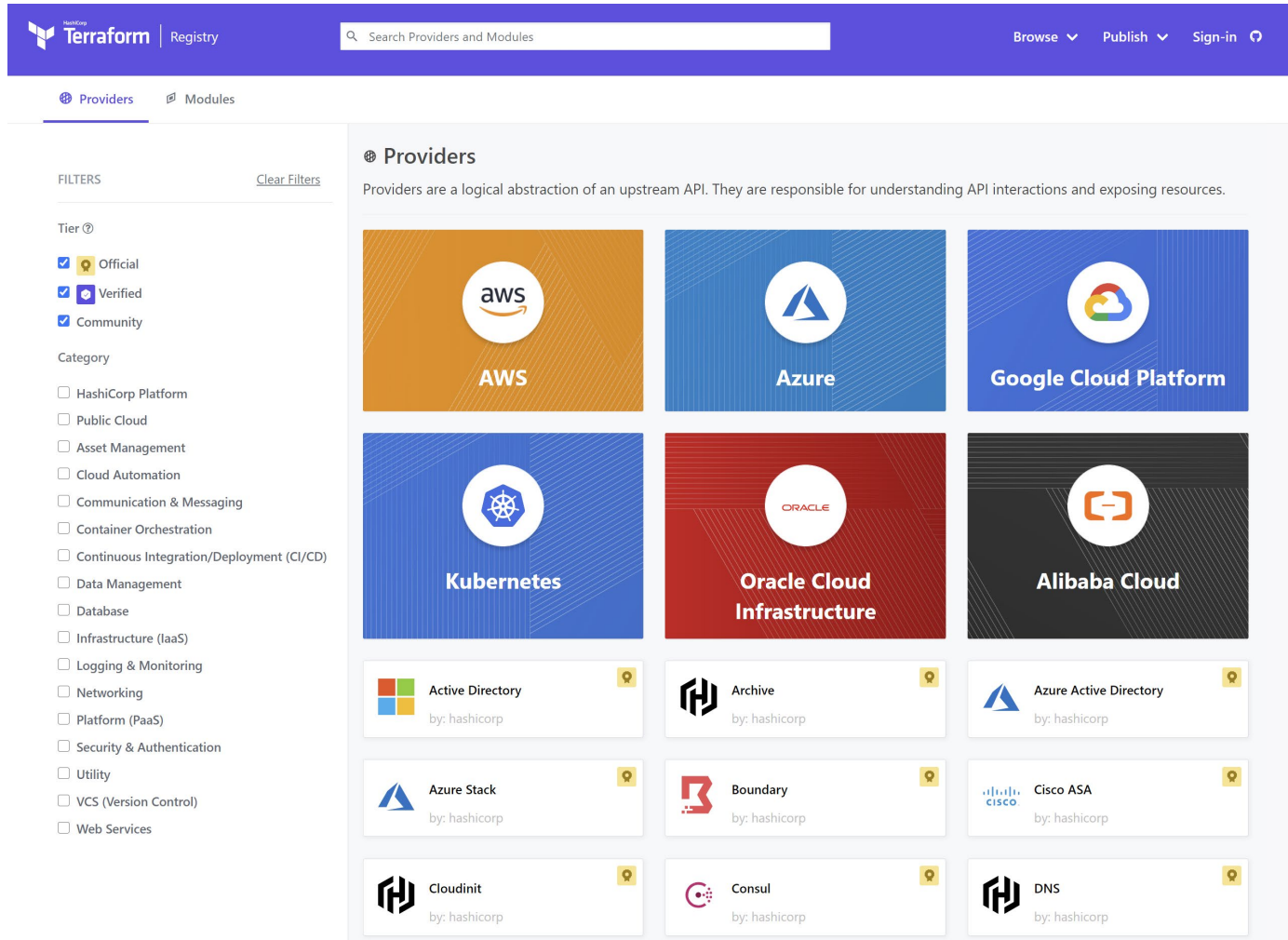
Terraform

# Infrastructure as Code



## Providers

<https://registry.terraform.io/browse/providers>



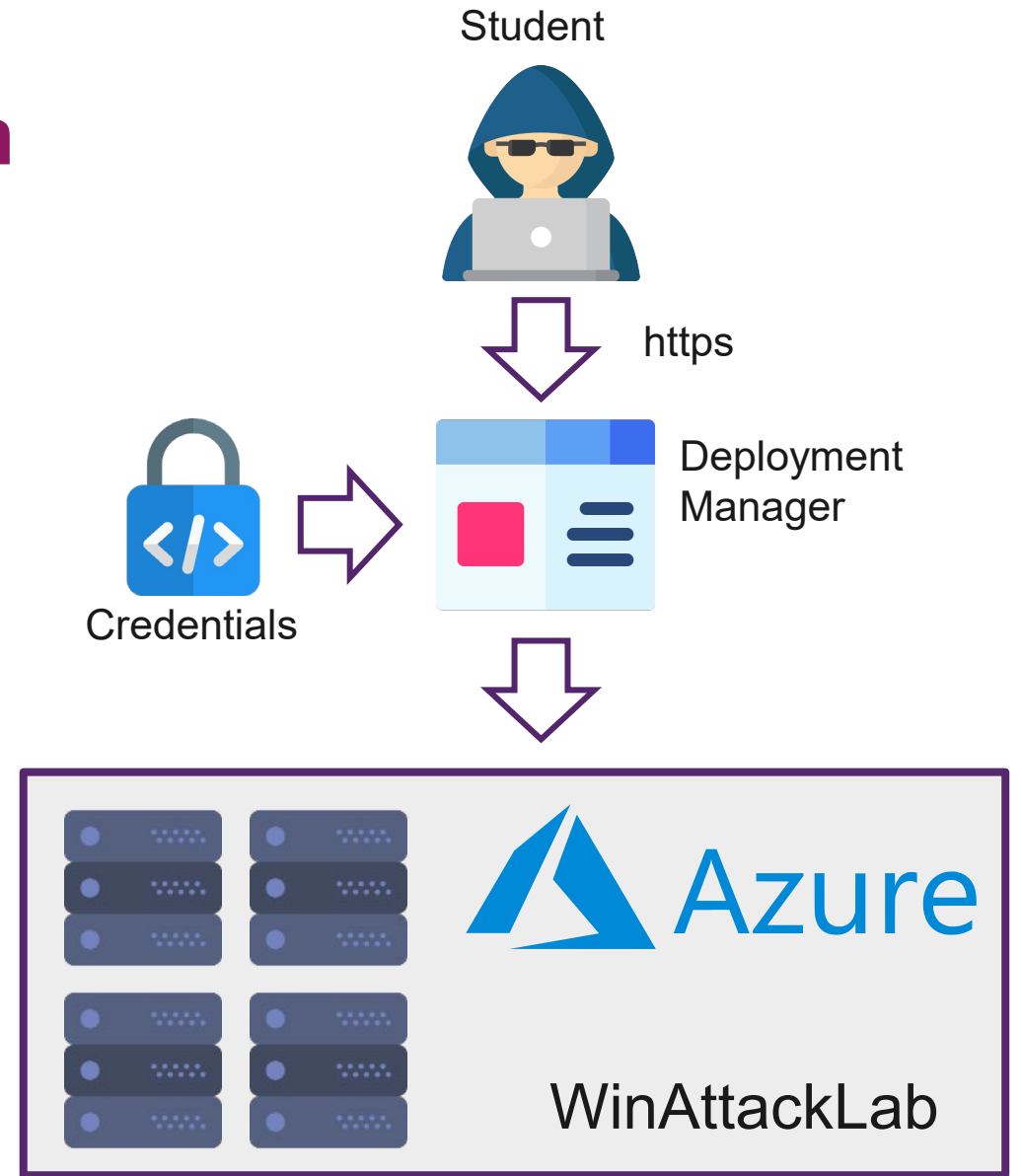
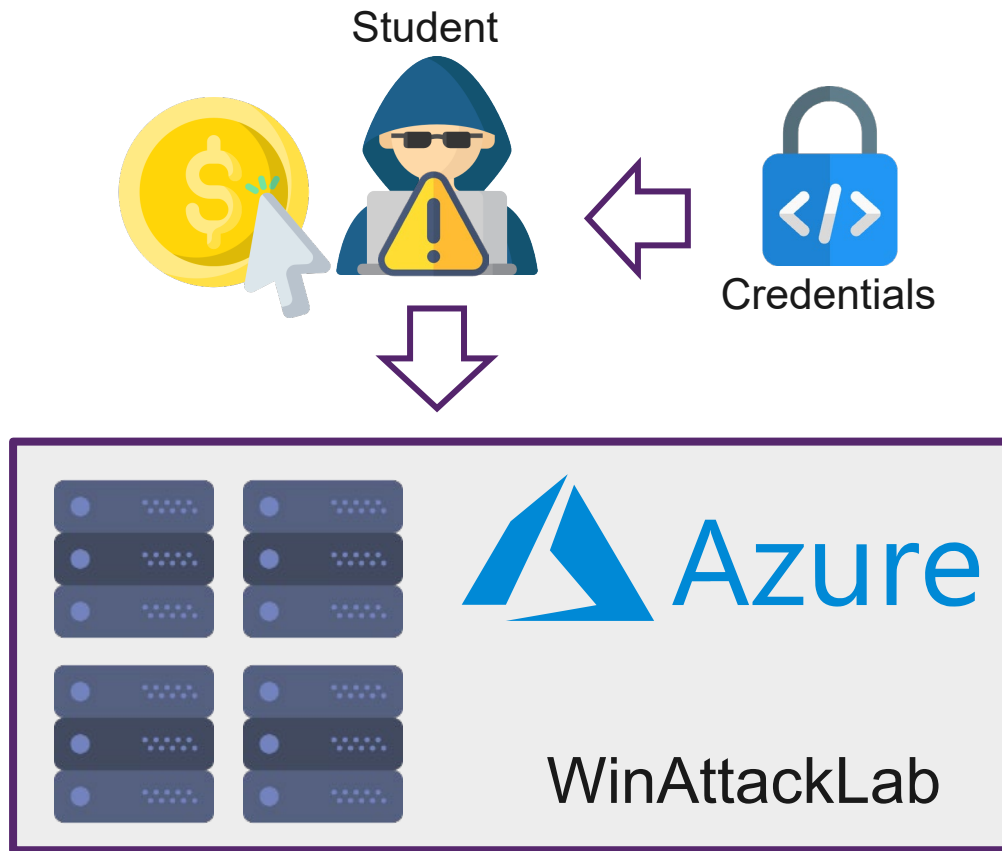
The screenshot shows the Terraform Registry Providers page. The header is purple with the Terraform logo, a search bar, and links for Browse, Publish, and Sign-in. Below the header, there are tabs for Providers and Modules. The left sidebar contains filters for Tier (Official, Verified, Community) and Category (HashiCorp Platform, Public Cloud, Asset Management, Cloud Automation, Communication & Messaging, Container Orchestration, Continuous Integration/Deployment (CI/CD), Data Management, Database, Infrastructure (IaaS), Logging & Monitoring, Networking, Platform (PaaS), Security & Authentication, Utility, VCS (Version Control), Web Services). The main content area is titled "Providers" and includes a description: "Providers are a logical abstraction of an upstream API. They are responsible for understanding API interactions and exposing resources." Below this, there is a grid of provider cards. The first row contains AWS, Azure, and Google Cloud Platform. The second row contains Kubernetes, Oracle Cloud Infrastructure, and Alibaba Cloud. The third row contains Active Directory, Archive, and Azure Active Directory. The fourth row contains Azure Stack, Boundary, and Cisco ASA. The fifth row contains Cloudinit, Consul, and DNS. Each card features the provider's logo and name.

**Providers**

Providers are a logical abstraction of an upstream API. They are responsible for understanding API interactions and exposing resources.

- AWS
- Azure
- Google Cloud Platform
- Kubernetes
- Oracle Cloud Infrastructure
- Alibaba Cloud
- Active Directory
- Archive
- Azure Active Directory
- Azure Stack
- Boundary
- Cisco ASA
- Cloudinit
- Consul
- DNS

# Credentials Azure Subscription

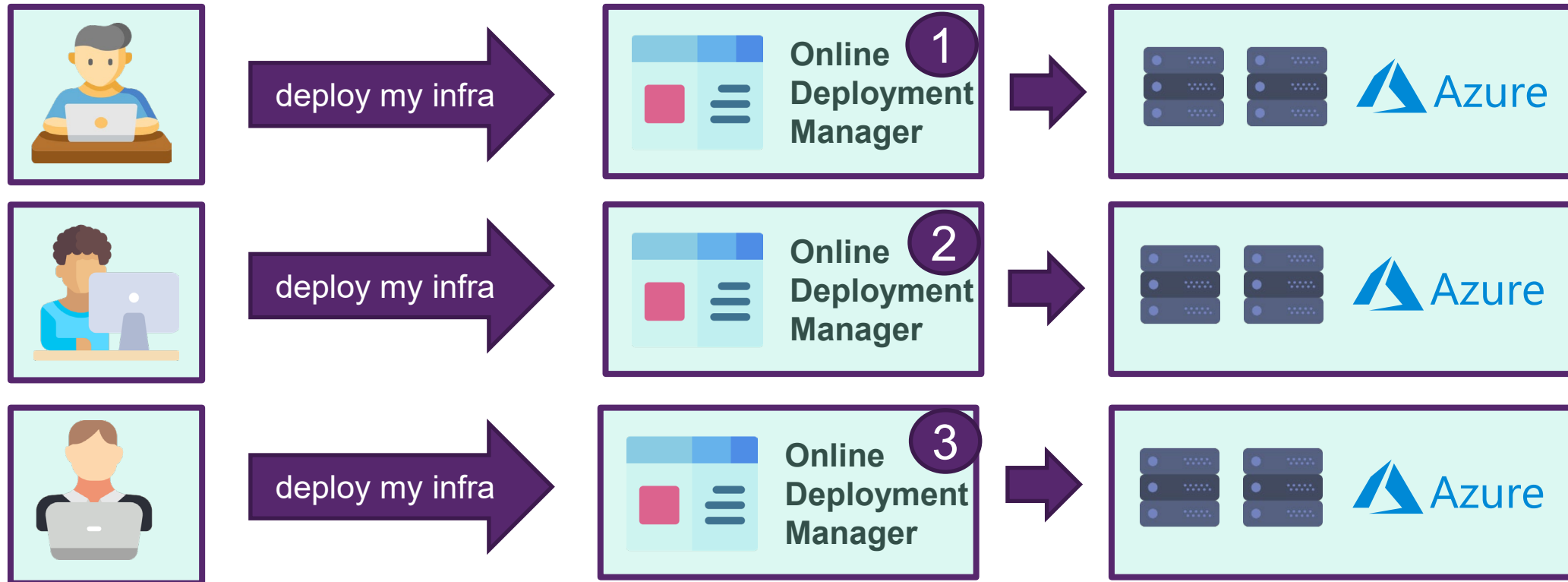


# Deployment Manager

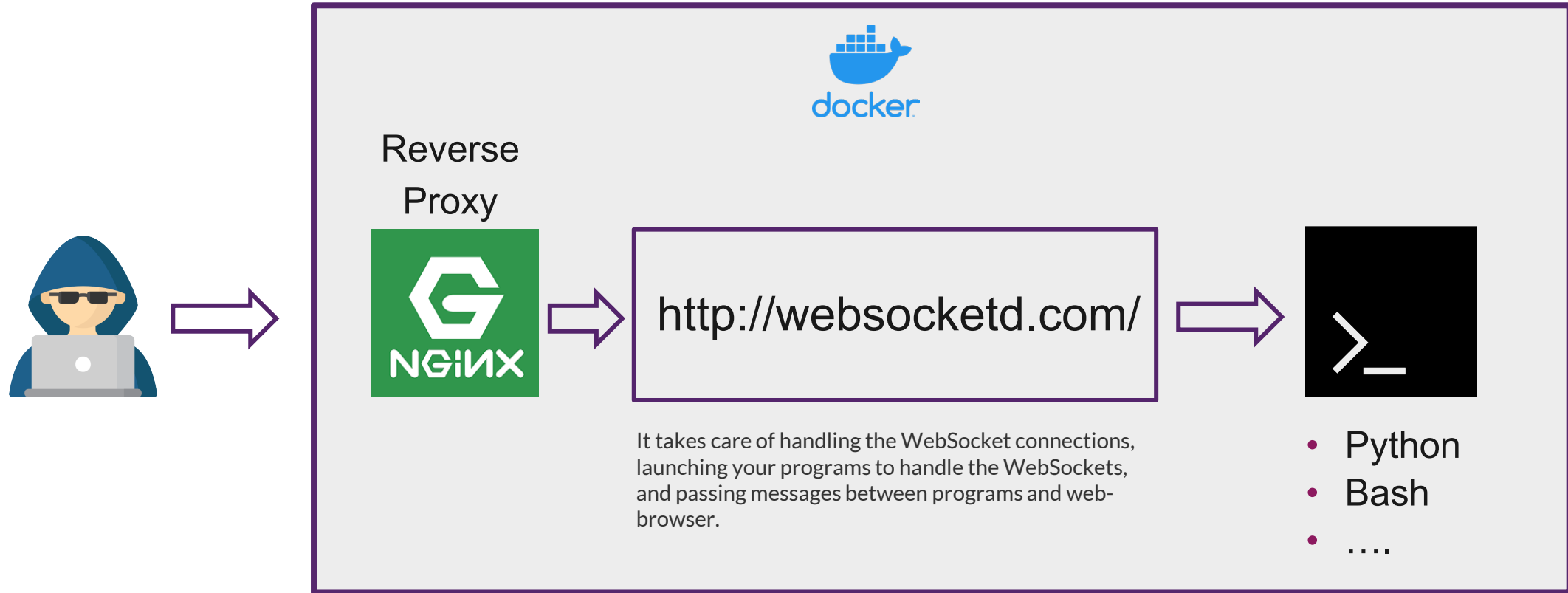
The screenshot shows the WinAttackLab interface. On the left is a sidebar with a blue header 'WinAttackLab' and four menu items: 'Deploy' (with a paper plane icon), 'Destroy' (with a target icon), 'Log' (with a list icon), and 'IP Addresses' (with a hexagon icon). A purple bracket groups these four items, with an arrow pointing to an oval labeled 'read-only'. The main content area has a blue header 'Deploy'. Below it is a terminal window showing the following text: 'CONNECT', 'Sun Nov 29 10:29:15 UTC 2020: terraform deploy not yet startet', 'Sun Nov 29 10:29:15 UTC 2020: if you want to start deploying, click on the "Run Task" button', and 'DISCONNECT'. To the right of the terminal is a blue button labeled 'Run Task'. A purple arrow points from an oval labeled 'change state' to the 'Run Task' button.

# Deployment Manager

## Scaling Up



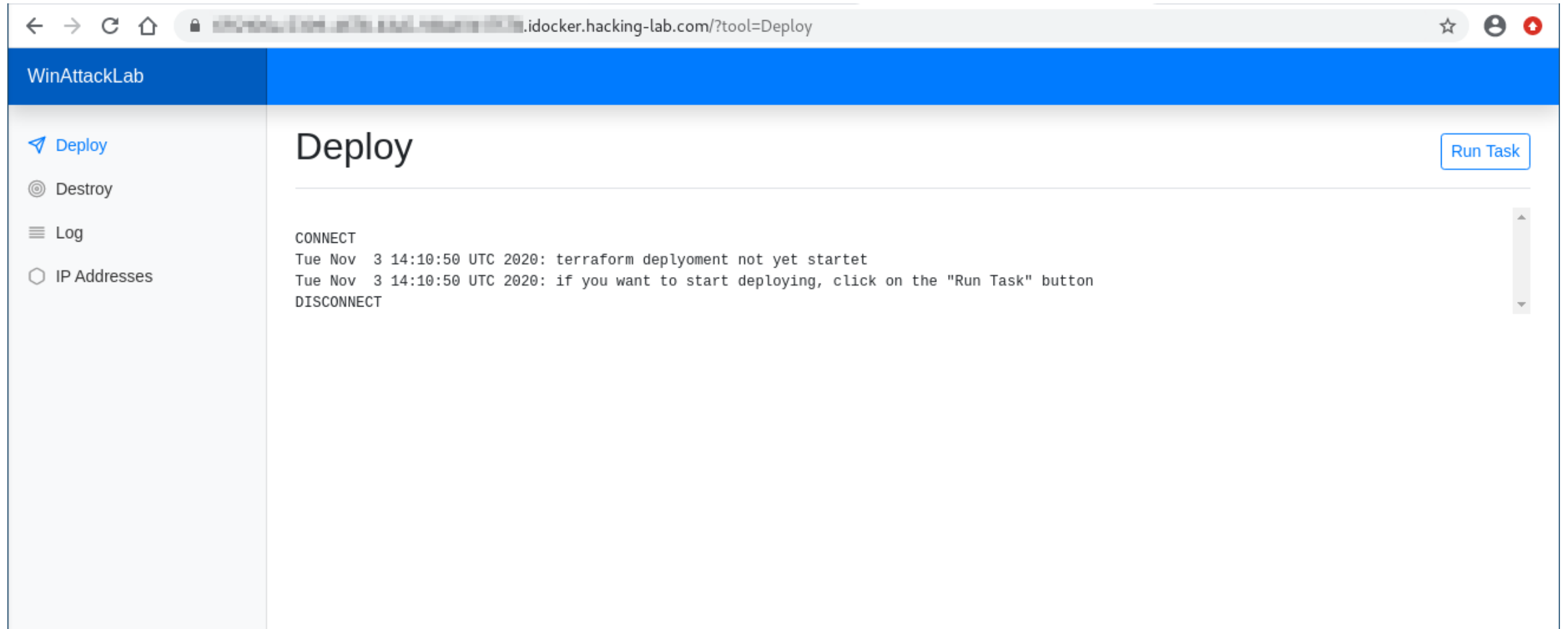
# Deployment Manager is based on «websocketd»



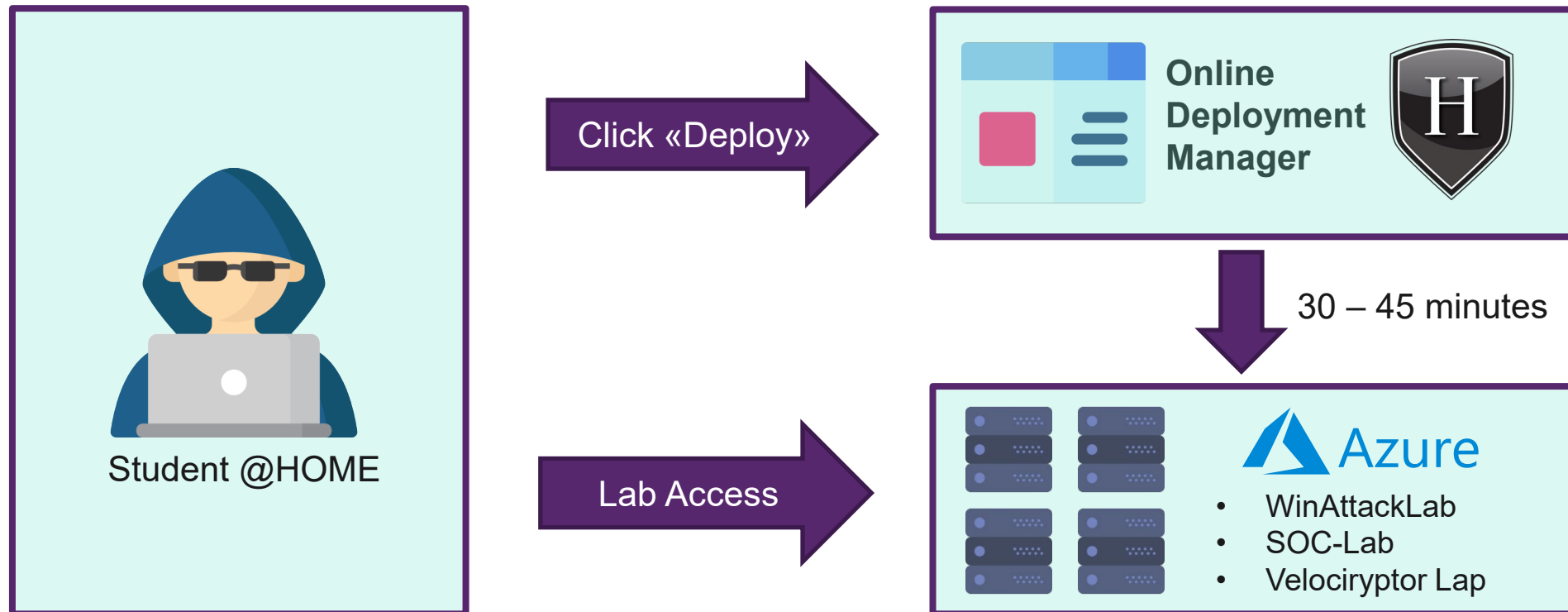
# How to use the Deployment Manager



# Deployment Manager



# On-Demand Deployment



## Login Credentials

- Click on «IP Addresses»
- Click on «Run Task»
- Login Credentials will be listed
  - Win10 Client (RDP)
  - Kali SSH
  - .... (others if required)

WinAttackLab

Deploy  
Destroy  
Log  
**IP Addresses**

IP Addresses

Run Task

```
CONNECT
Fri May 7 05:31:34 UTC 2021: terraform is fully deployed
Fri May 7 05:31:34 UTC 2021: user did not click on destroy
===== Azure Resource Group =====
SOC_KaliVM_41nu
=====
kali_public_ip = "20.71.63.102"
management_public_ip = "13.95.88.68"
winclient1_public_ip = "20.71.61.42"
=====
Fri May 7 05:31:37 UTC 2021: infrastructure will automatically destroy in 39479 seconds
Fri May 7 05:31:37 UTC 2021: infrastructure will automatically destroy on Fri May 7 16:29:36 UTC 2021
===== PUBLIC IP ADDRESSES =====
kali_public_ip = "20.71.63.102"
management_public_ip = "13.95.88.68"
winclient1_public_ip = "20.71.61.42"
===== Win10 Client RDP Access =====
Protocol: RDP with username/password authentication
Server: "20.71.61.42"
Domain: winattacklab.local
Username: tmassie
Password: WinLAB!123
===== Active Directory =====
Server: dc1.winattacklab.local
Server: 10.0.1.100
DC Username: lab_admin
DC Password: 7e315ddc-de98-4ec5-ab45-0adb3ee71f1c
===
===== Kali SSH Access =====
Protocol: SSH with publickey authentication
Server: "20.71.63.102"
Username: lab_admin
Password: 242b12e6-ad13-46ce-b6a8-6afc22e603a6
===
Password: see ssh private key below
Command: ssh -i /ssh/kali-private-key lab_admin@20.71.63.102
```

find the Win10 RDP login credentials here

# Access to the Lab

## Windows 10 Client

- Access via RDP (use **remmina** on livecd)
- IP: **<get from deployment manager>**
- Username: tmassie
- Password: **<get pw from deployment manager>**
- Domain: winattacklab.local
- Privileges: Regular domain account

Basic	Advanced	Autostart	SSH Tunnel
Server	52.166.69.184		
Username	tmassie		
Password	••••••••		
Domain	winattacklab.local		
Resolution	<input checked="" type="radio"/> Use initial window size <input type="radio"/> Custom 640x480		
Colour depth	GFX AVC444 (32 bpp)		
Share folder	<input checked="" type="checkbox"/> tmp		

your IP address

map a local folder

## Linux Attack Host (Kali)

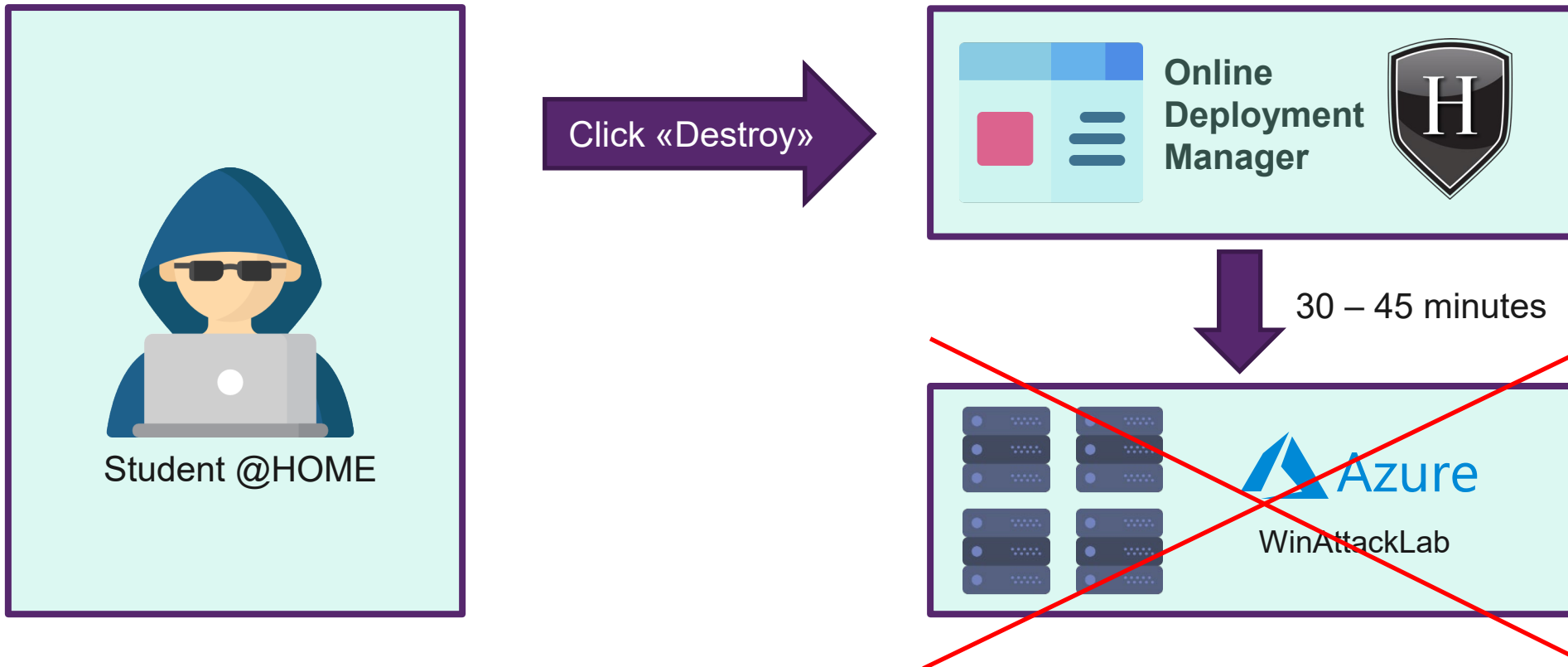
- Access via SSH
- IP: **<get ip from deployment manager>**
- Username: lab\_admin
- SSH private key: **<get key from deployment manager>**
- SSH passphrase: **<not set>**
- Privileges on Kali Linux: root (with sudo)

```
root@kali:~# ssh -l lab_admin -i ./ssh-key <ip>
Linux kali1 4.19.0-kali4-amd64 #1 SMP Debian 4.19.28-2
kali1 (2019-03-18) x86_64

[CUT BY COMPASS]

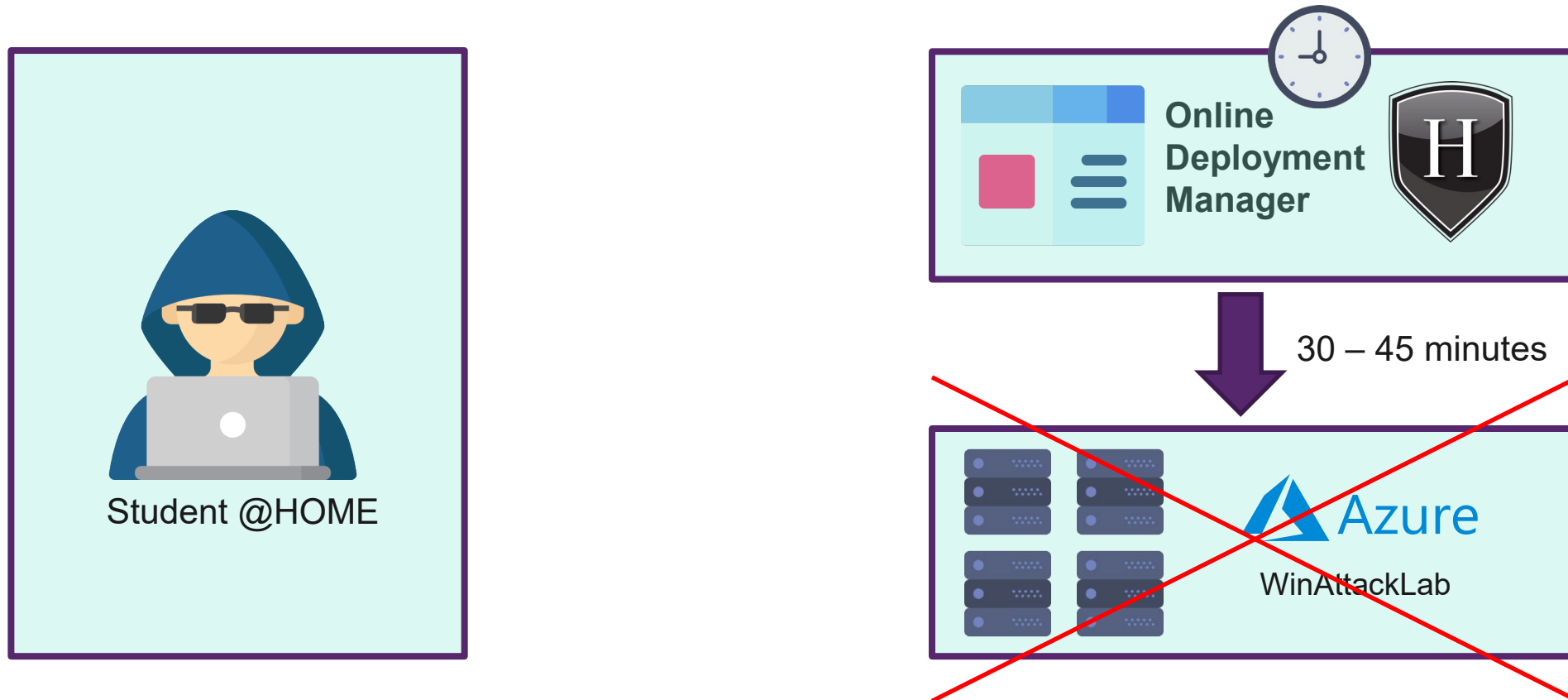
Last login: Fri Feb  7 05:42:11 2020 from 146.4.10.235
lab_admin@kali1:~$
```

## On-Demand Shutdown



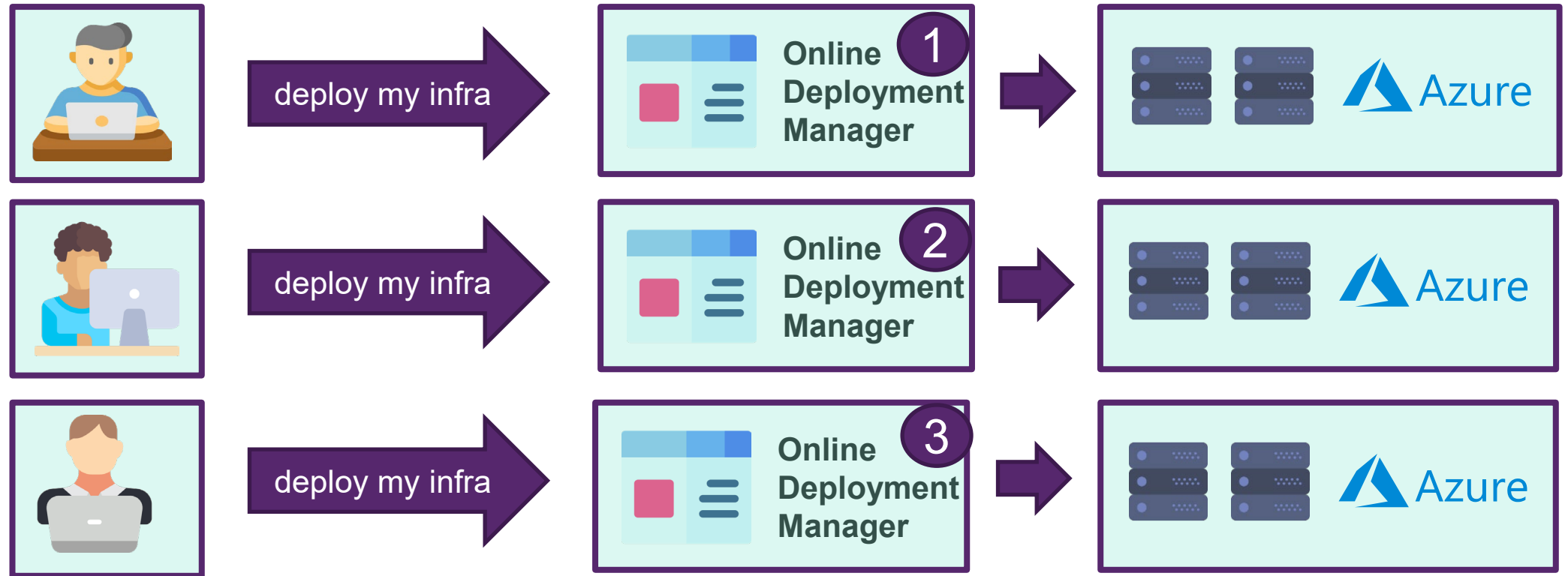
The lab will fully destroy and you will loose all your changes once it is destroyed

## Automatic Shutdown after 8 hours



The lab will fully destroy and you will loose all your changes once it is destroyed

# Deployment Manager per Team



Every team can use it's own lab – independend from the other teams!



# 2-er Team

- Please make teams (2-3 persons per team)
- Start the lab 1hour prior starting your lab session
- Start the lab via Deployment Manager
- **Stop** the lab at the **end of your lab session** (saving costs)
- Otherwise, the lab will automatically destroy after 8 hours (from when you clicked «Deploy»)