azure-pentesting-lab-tf

Matt Burns | October 2, 2022

Prerequisites:
- Create Azure Student account
- Install Azure CLI
- Install Terraform
- Install Microsoft Remote Desktop

Build:
- Clone Git repository
- cd azure-pentesting-lab-tf
- terraform init
- terraform apply

Access:
- After Terraform has built the resources, it will output the IP addresses of the two hosts in the Public Subnet
- Open the Remote Desktop application
  - **Windows:** Start > type "mstsc"
  - **Mac:** Applications > Microsoft Remote Desktop
- RDP to the IP output by Terraform after it's finished building the resources

Student Home Network

Student PC → RDP Client
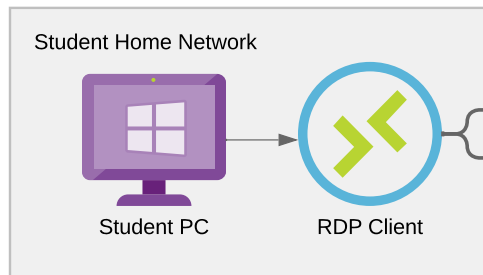
Hosts:
LIN-KALI-PUB
- Public Kali Bastion Host
- Access via RDP (Public IP will be output to the terminal when Terraform finishes building resources)

WIN-HOST-PUB
- Public Windows Bastion Host
- Access via RDP (Public IP will be output to the terminal when Terraform finishes building resources)

WIN-SERV-PRI
- Private Windows Server, access through bastions
- Includes Nessus. Access UI from Bastion by navigating to 10.0.2.5:8834

WIN-HOST-PRI
- Private Windows Host, access through bastions

LIN-SYON-PRI
- Private Security Onion Host
- Access the UI from Bastion (10.0.2.15)

LIN-VULN-PRI
- Vulnerable Linux host (attack from KALI Bastion)

Azure

Student's Azure Subscription

Virtual Network (10.0.0.0/16)

Public Subnet (10.0.1.0/24)

LIN-KALI-PUB
Kali VM
10.0.1.5

WIN-HOST-PUB
Windows Host
10.0.1.10

Private Subnet (10.0.0.2.0/24)

WIN-SERV-PRI
Windows Server
10.0.2.5

WIN-HOST-PRI
Windows Host
10.0.2.10

LIN-SYON-PRI
Security Onion VM
10.0.2.15

LIN-VULN-PRI
Metasploitable VM
10.0.2.20