# Threat Hunting Lab Environment

Having a lab or research environment available for hunters is a critical component of a effective threat hunting program. The OTHF Threat Hunting Process touches briefing on lab environments during the “Create Test Data” section of the process however in this section, we will cover some fantastic tools to help hunters build threat hunt lab environments of various scales.

## Blue Cloud

BlueCloud is a collection of Terraform and Ansible scripts that enables users to deploy a cyber range within AWS or Azure.

GitHub Repo: <https://github.com/iknowjason/BlueCloud#infrastructure-and-credentials>

Documentation: <https://blue.iknowjason.io/>

## OTHF Hunting Lab

The OTHF team has put together a collection of Vagrant files that enables users to build a small Microsoft Active Directory environment with a domain controller, member servers, and workstations with all endpoint logs being sent to a Splunk server.

OTHF Lab Credentials

Domain Administrator:

Username: Administrator

Password: !P@ssword123456

Domain: OTHF.local

Local Windows Credentials:

Username: vagrant

Password: vagrant

Splunk:

Username: Admin

Password: Vagrant123

### Building

Prerequisites:

Virtual Box

Vagrant

vagrant plugin install vagrant-windows-domain

vagrant plugin install reload

Build

Provision Domain Controller

* From a command prompt navigate to BuildDC directory and type “vagrant up”
* Once provisioned, log into the new VM with Username: Vagrant Password: vagrant
* Open PowerShell as Administrator and run InstallDomain\_1.ps1 from c:\users\vagrant\desktop
* When completed, restart the domain controller
* Note: double check that Adapter 2 is on VirtualBox host-only ethernet adapter sometimes VBox will create multiple adapters.
* Log into the domain controller with username: othf\administrator password: !P@ssword123456
* Open PowerShell as Administrator and run InstallDHCP\_2.ps1 from c:\users\vagrant\desktop, when prompted type Y
* At this point, you should have a Domain OTHF where the domain controller IP is 10.10.1.1 on Ethernet 2 (host only), a DNS record for dc1 for 10.10.1.1, and DHCP server serving up Ips in the 10.10.1.0/24 space

Provision Splunk

* From a command prompt navigate to Splunk directory and type “vagrant up”
* Note: double check that Adapter 2 is on VirtualBox host-only ethernet adapter sometimes VBox will create multiple adapters.
* When finished, log into the Splunk server using username: vagrant password: vagrant
* Configure the Splunk server w/ the IP address 10.10.1.3
* Open firefox, and navigate to http://127.0.0.1 :8000
* The splunk UI should appear, log in with username: admin password: Vagrant123

Provision Workstation/Server:

* From a command prompt navigate to Splunk directory and type “vagrant up”
* Note: double check that Adapter 2 is on VirtualBox host-only ethernet adapter sometimes VBox will create multiple adapters.
* When completed reboot the machine.
* Log in and navigate to c:\\users\\vagrant\\desktop\\ConfigAuditing.ps1 and run as administrator

Once all the components are built, you will have Sysmon and Windows Event Logs flowing to Splunk in the index “threathunt”

To search

* Open firefox, and navigate to http://127.0.0.1 :8000
* The splunk UI should appear, log in with username: admin password: Vagrant123
* Click on search and reporting
* Type in index=threathunt and look in the past 15 minutes to view logs