Cyber Night Pro Talk

Tips, Tools, Tricks and Treats for Cybersecurity

Presenters:

Alex Lafrenz – OWASP

Eric Crutchlow – Tenable

Jase Kasperowicz – Crowdstrike

Brandon Brown – Coastline College

Setting up your very own @Home LAB Environment

Tools tips and tricks to help teach yourself Hands-On Cybersecuirty

Brandon R. Brown PhD
Coastline College

Some Pre-Requisites

- This can be an expensive industry to break into.
- Compute Power is at a premium
- Most employers will afford their security staff top tier equipment
  - TAKE ADVANTAGE OF THIS!
- Leverage Cloud Services
  - AWS
  - Google
  - Azure

The Virtual Environment

- VMware vs. VirtualBox
  - VMware
  - VirtualBox
- Alternate Virtual Environments
  - GNS3
  - Cisco Packet Tracer

YouTube is your Friend!

When first learning anything cyber, remember, someone before you probably learned it too and made a YouTube Video about it!

Bonus! – This will also perfect your Google Hacking / Searching Skills!

Old School Trick!

- Don’t limit yourself to YouTube
- There are plenty of plain text guides as well.
- Some even have pictures!
- Beware, they are not always right.

Cloud is Free*

- * Sort of…..
  - Keep in mind that cloud providers are out to make money. It is all about learning HOW they make money and skirting around it.
  - For Example – Public IPs in AWS (Elastic IPs)
    - Charged at $0.02 / hr.
    - While in use it is Free?
    - Buyer beware please…..

Cloud Uses

- Virtual Private Clouds
  - Here you can setup your own internal environment for testing / development
  - Lots of good and free compute space you can use.
- Caveat! You need to be good at some development because the OS in these services are pretty hardened already

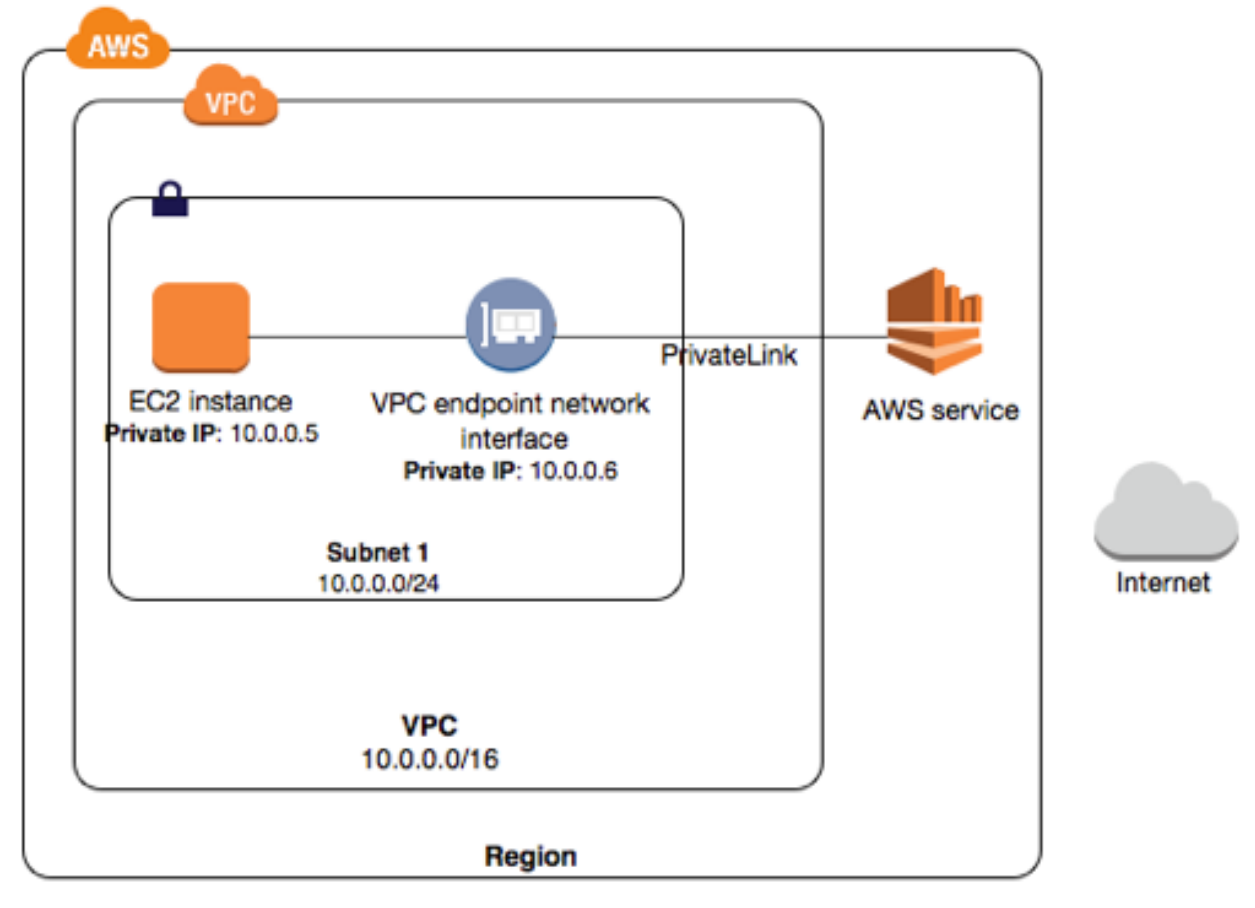
Cloud Cont.

- If you are going to use cloud, be sure you know how to import your own VMs.
- This can be done in AWS.
  - Link to VM import / export AWS.
  - Link to import in Google Cloud
  - At this time, Azure does not have a way to import all VM types, Only Hyper-V

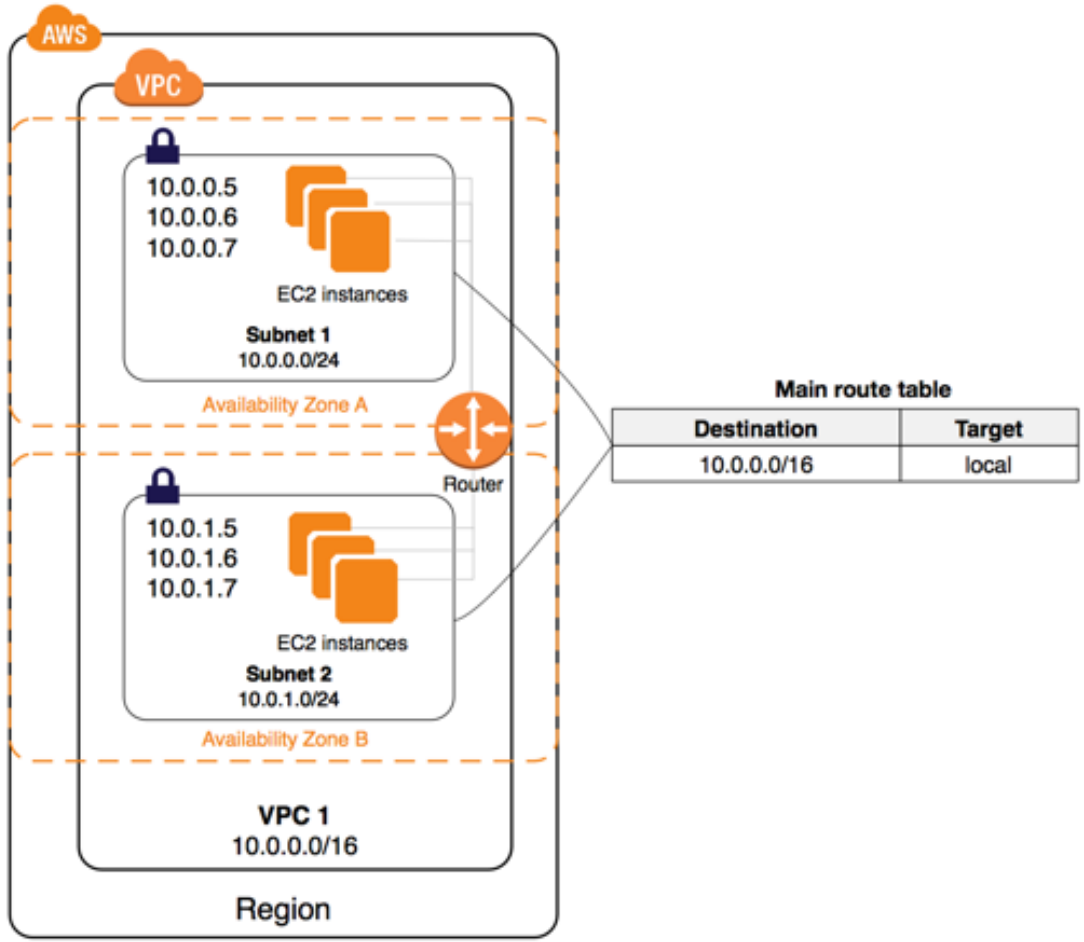
Understanding Networking

- Regardless of Virtual Environment Type
  - You must have some networking background
- VMware
  - Player / Workstation
  - ESXi / Vsphere
- AWS VPCs

VPC Example - 1



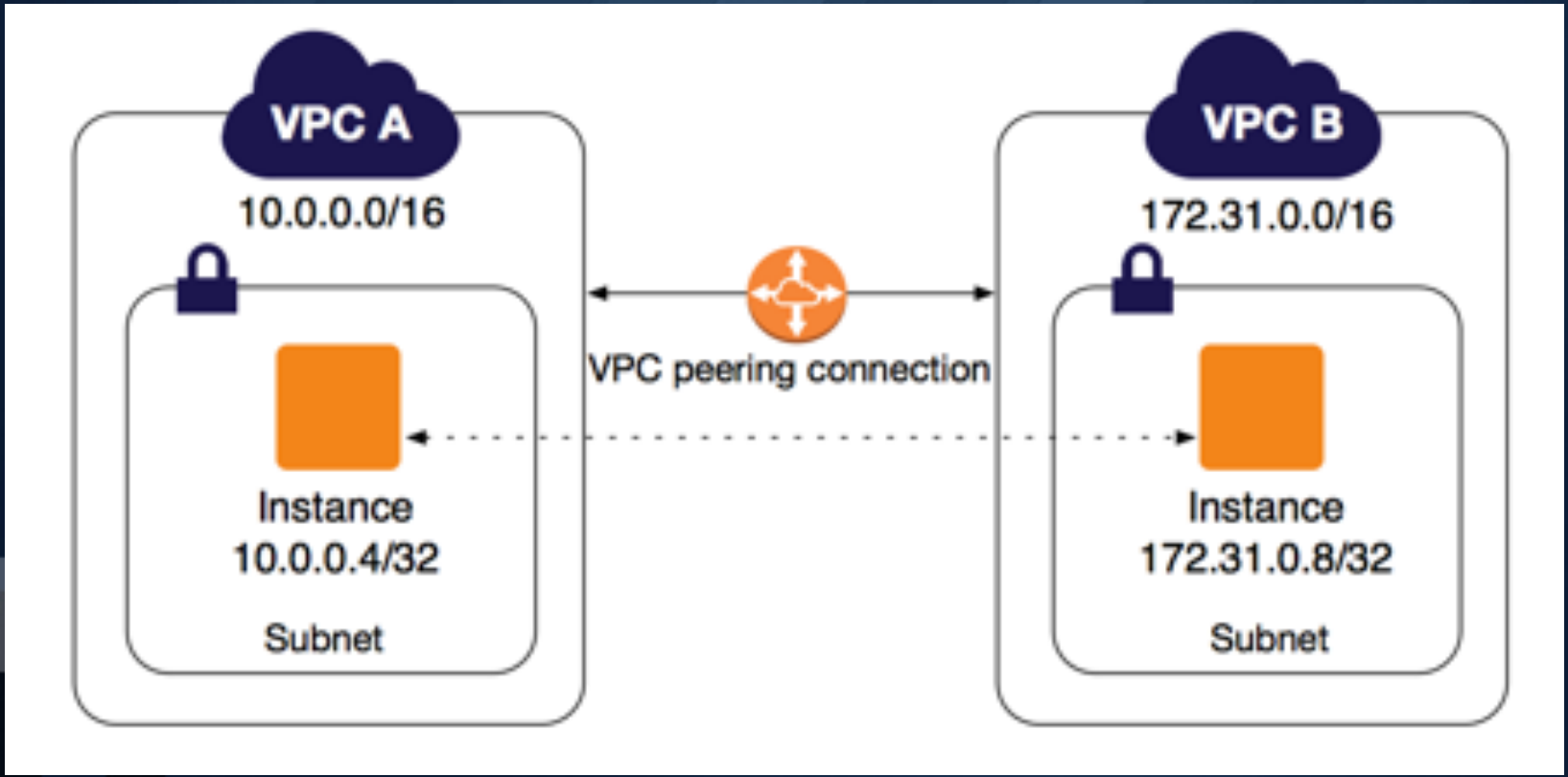
VPC Example - 2



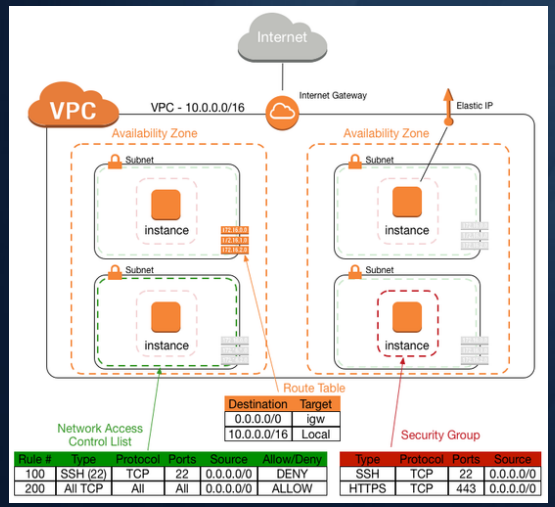
Main route table

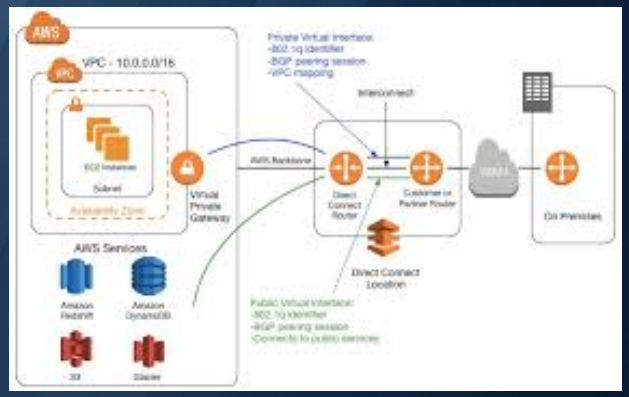
Destination	Target
10.0.0.0/16	local

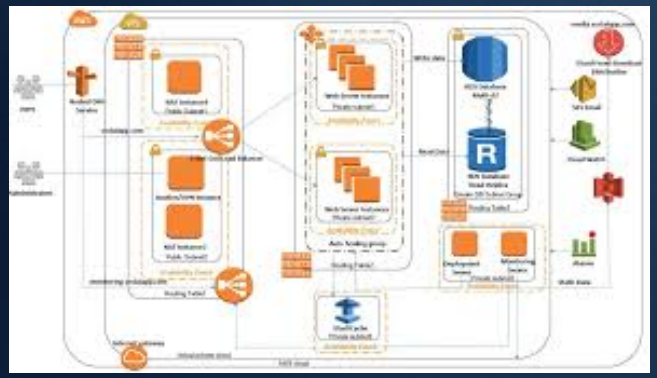
VPC Example - 3

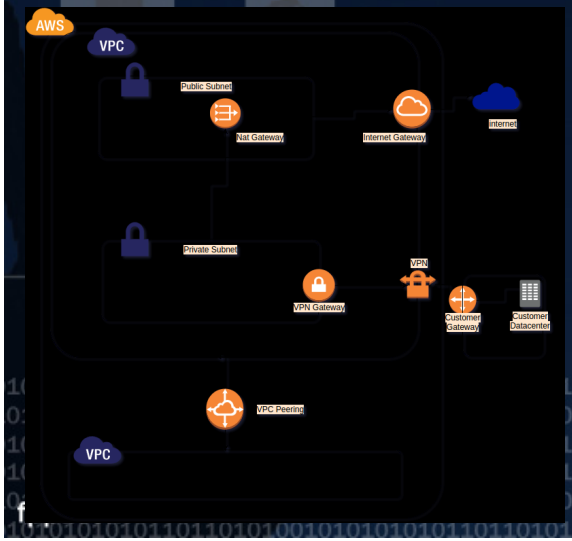


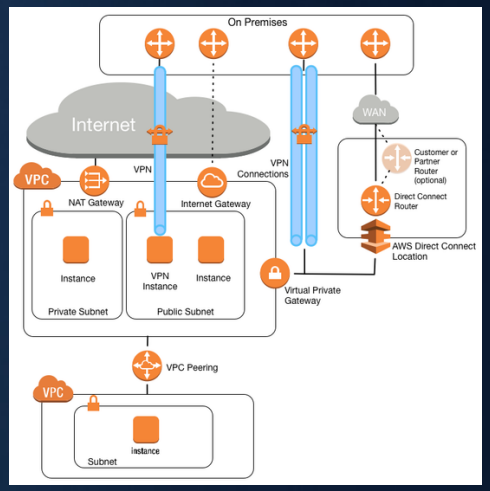
VPC Example - X











It looks complex. But try to keep it Simple

- Start off with VMware if you can.
- Build out your core
  - Kali
  - Parrot OS
  - Windows Ninja
- Start with simple tools.
- Most offensive security experts struggle with the networking portion first.

Keeping it simple cont.

- Understand which platform uses which gateway
- Learn how to used internal networking in your host OS (Windows or Linux)
- Don’t be afraid to “Air Gap” your system
- Ping is your BFF!
- You can’t hack if you can’t access your target.

A quick Demo

- Here is a look at my system…

Thank you and Good Night!