The Host Machines

The next step in the home lab journey is to provision our host machines. This section will include a Windows 10 Pro image, an Ubuntu 22.04 image, and a vulnerable Windows 10 Pro image with numerous security issues. All three of these machines will be domain joined and connected to the NAT-ed network. I chose this setup for a bit of differentiation and to cover the bases of what kinds of machines will be in an enterprise network.

The first Windows 10 Pro image is just a basic installation of Windows. I started with this because I wanted to make sure that DHCP was configured and functioning correctly. I was having some trouble at first with DHCP because the VM was not being given an IP address in the range that I specified. I realized that I did not have the Domain Controller powered on before I provisioned the VM. Obviously, DHCP cannot assign an IP address if it is not active. Once I got over this little hurdle, I checked the address leases in DHCP to make sure everything was connected correctly, which it was. Finally, I checked the “Computers” section in Active Directory to verify that the machine was domain joined.

The next machine I provisioned was an Ubuntu 22.04 image. To make this environment as realistic as possible, I wanted to include a Linux machine that I could also join to the domain. Provisioning the VM is pretty straightforward, but joining a linux machine to an AD domain takes some extra steps. To make this possible, we need to install SSSD, which is a set of daemons that allows you to remotely access directories and authentication mechanisms. The steps include updating your system, setting a hostname, installing the packages, finding the AD domain, and joining the domain (guide to connecting listed in Resources). Also, Nessus Essentials will live on this VM and run scans from this internal location.

The next order of business was to provision a vulnerable machine to be a target for vulnerability scanning on the network. Originally, I wanted to provision a Windows XP machine, but finding an ISO for that proved to be impossible. I decided to just spin up a Windows 10 VM and disable all of the security features. The process for provisioning the machine is the same as any other Windows 10 machine, but I disabled Windows Defender and turned off all firewall rules. Finally, I uninstalled the latest Windows update. This should be more than enough for the vulnerability scanner to pick up and analyze the results.

The SIEM will need a couple of VMs for it to function as intended. In order to make Splunk work how I envisioned it, I need to spin up a VM for the Splunk service and another for the universal forwarder. I decided to use Ubuntu for both of these machines because Splunk wasn't too difficult to download and I like to try and keep things consistent where I can. We will get more into the setup in the Security Services document.

The final host that needs to be provisioned is yet another Windows 10 Pro VM. This will serve as the "RDP server", even though it is not running a server OS. This is basically just another machine with RDP enabled so we can RDP into other machines, like our Domain Controller. There is nothing fancy to configure here, other than enabling remote access on any machine that you would like to remote into. Even though this is not necessarily a true "RDP server", I wanted to be able to configure/secure RDP, which will be discussed in a later project.

Resources

Join Ubuntu to AD Domain

https://computingforgeeks.com/join-ubuntu-debian-to-active-directory-ad-domain/

Configuring the Correct Network Connection in VMware

https://docs.vmware.com/en/VMware-Workstation-Player-for-Linux/17.0/com.vmware.player.linux.using.doc/GUID-FC54BCB2-9529-4FA8-9BD7-613BFFD4E103.html