Documentation for the Active Directory/Splunk project

1. I started by creating a diagram, using draw.io. This diagram includes the scope of our project and shows the flow of data over our network of virtual computers.

This diagram can also be viewed separately as ActiveDirectoryLab.io

2.The next step was to download and create 4 virtual machines. I downloaded .iso files for Windows 10, Windows Server 2022 and Ubuntu 22.04, and spun up three VMs in Virtual Box. I also downloaded a prebuilt Kali Machine for VirtualBox and installed that well.

3. Its time to download and install software onto these devices. I began by ensuring that the computers on my virtual network could all communicate with each other and the internet. I created a NATNetwork in VirtualBox and configured all of our devices to be a part of it. To set up our splunk server we need to disable DHCP, set a static ip address, default router and configure which DNS server to use. To do this I edited the .yaml configuration file. I created a shared directory in virtualBox to use for this lab, and downloaded splunk into it. Added dependencies for Virtualbox interactions and then mounted a folder i created in ubuntu named ‘share’ to the directory i created for this network named “WindowsActiveDirectory”. From here I downloaded the splunk installer onto my VM. Configured splunk through the installer and set splunk to start up on system boot.

Checked in with my dashboard at this point and I do have a fully functional splunk instance. There was a problem accessing the dashboard with the host device, but this was fixed by setting a port forwarding rule in virtualBox.

4. Now it is time to download the universal forwarders onto the Active Directory and target device(windows 10). First I ensured my VM was correctly configured and set up with my network, I set a static ip address, confirmed the dns server and set a confirmed router. From the browser I downloaded the splunk forwarding agent and sysmon, along with a sysmon configuration file. I used the installer and configuration file to install sysmon. I also created a new inputs.conf for the splunk forwarder to make sure it is forwarding the correct information to the splunk instance.

This telemetry is being sent to an index called “endpoint” which I created in splunk.

At this point, it is time to check if I am seeing events the splunk index. And I am!!! 6,000 events to the new index “endpoint” which are coming from the Windows 10 forwarder. I followed a similar process to install a forwarder on the Active Directory Server. I needed to be sure to set a deployment server as the Active Directory server in this step. After installation, I revisited the Splunk dashboard and find that Splunk is receiving telemetry from both devices. I also set a static ip address for the Windows Active Directory server at this point.

5.Now, its time to install and configure Active Directory on the AD server, soon to be domain controller. Utilizing the ‘Add Roles or Features’ section of the server manager, I began a ‘role or feature based installation’ I followed the prompts until I could select ‘Active Directory Domain Services’. Followed the prompts through and waited. At the end of the installation I received a notification that I need to configure the Active directory server as a Domain Controller. I followed the prompts. Made sure to name the domain with a top level domain name. This means it need to be composed a “.anything”. For ease of use and fun with users later I named our domain “THESHIRE.LOCAL” Followed the prompts through, not much to change for my current needs. At this conjecture, our device will automatically restart. We log back in and find that we see our domain followed by a “\” in this case THESHIRE\administrator. Now its time to make some users. We create a few groups in Active Directory for experimental purposes, for the example, i used “Hobbits” and “Wizards”. I also added a few users at this point “Frodo Baggins:fbaggins” and “Gandalf TheGrey:gthegrey” and set their passwords to ones that will be somewhat easy to guess, for use later in the lab. Just like that I configured the Active Directory Server. Now its time to set up the Agent!

6. On the windows 10 machine I needed to modify the properties of our pc. Namely I needed to modify the PC’s name to include a domain name, to connect with the Active Directory server. This can be done through advanced system settings under the properties of ThisPC. I modified the name, making sure to check the box for “Domain Name” and add in the new domain “THESHIRE.LOCAL”. At this point, the agent does not know how to resolve “THESHIRE.LOCAL”. I fixed this by changing the adapter settings. I modified the properties of the adapter, changed the settings under ipv4 address and modified the domain name services to point to the domain controller.

I double checked that the DNS are pointing to the Active directory by running ipconfig in the cmd prompt and checking the results. Going back to where I was renaming the device, I followed the GUI to change the domain to “THESHIRE.LOCAL” and this time it runs through a prompt, as it connects to the DC. I logged in with the administrator credentials for our DC as this account has the proper permissions. I followed the prompts, through to a restart. Upon logging back in I discovered that I have an ability to login as Other Users now. Under other users I can see that the domain name is there and I can provide credentials corresponding to the users of that domain. I entered the credentials for fbaggins from the previous step, and it works!

7. The final step! I need to verify that EVERYTHING works. I first configured the kali machine with the latest updates and download a tool named crowbar to perform brute force attacking. On the target machine, the Agent, I enabled the RDP for both users available in Active Directory server. And the fun begins. I ran a brute force attack utilizing the appropriate commands for crowbar and a simple wordlist that includes the passwords for both of the users on the AD server. A successful login! After running through the list the brute forcing tol has returned ‘fbaggins’ and the not so secure password as usable credentials.

8. Time to investigate the target device. I do this by using the new Splunk Dashboard. I searched the index “endpoint” for events occurring in the last 24 hours and I see alot of events!!! Upon further investigation I find 40 events pertaining to event code 4625!! This is a serious matter, I find out that some one is brute forcing the system. Upon further inspection I find some instances of event code 4624 They gained access as well! It looks like we need to tighten up our defenses but at least we can find the data easily with our SIEM.

9. At this stage I downloaded Atomic Red Team on to the target device so I can generate even more telemetry to analyze!!! In order to use Atomic Red Team, I needed to make an exception in the C:/ drive for Windows Defender. This is because there are some files that Defender will consider malicious and not allow to be downloaded. After creating the exception I used powershell with administrative privileges to download Atomic Red Team from GitHub and install it through the use of the packages from the download. After Atomic Red Team has been downloaded its time to generate even more telemetry. I cross referenced the MITRE ATTACK framework with some of the modules available in the Atomic Red Team program. I ran the program for creating a new local user with administrative privileges. Attackers would use this to create persistence in the system. Searching the logs I see alot of events pertaining to event code 4672. Upon further investigation we find out that this has to do with a new logon being assigned special privileges. So the Atomic Red Team experiment worked as well! Time to get cracking on figuring out how to defend better and to detect more threats.