**ITSC 301 – Wireless Security**

**Group Presentation Writeup**

Submitted by Coleton Sanheim

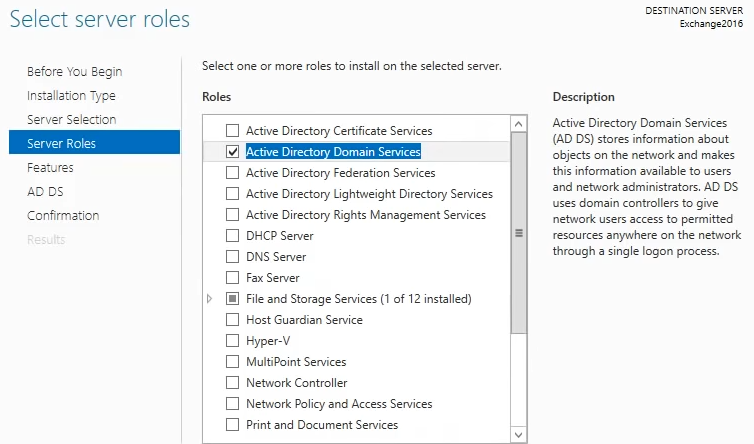
**Set up:**

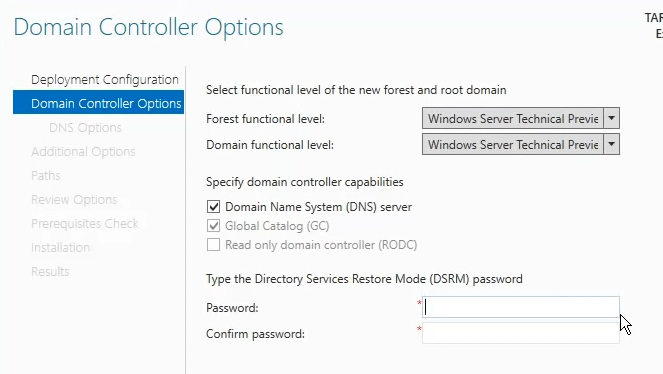
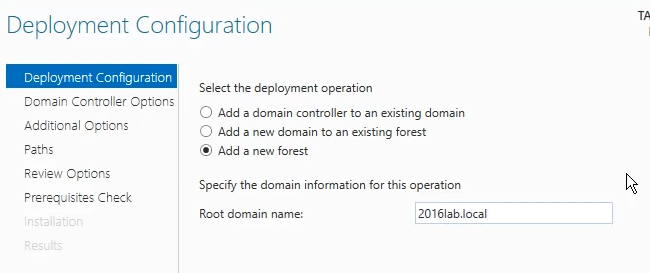
The proxyshell attack that we performed targeted a Microsoft exchange server so the first thing we need to do is to set one up.

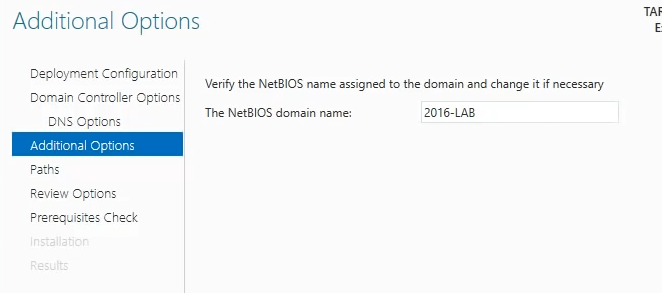
The first step is downloading a Microsoft 2016 server ISO and setting it up as a VM. Note that it has to be 2016 or earlier as later implementations such as 2019 have the vulnerability patched.

Once the server VM is ready the next step is configuring some settings, first up we need to set a static IPv4 address.

Next step is to set up Active Directory services.

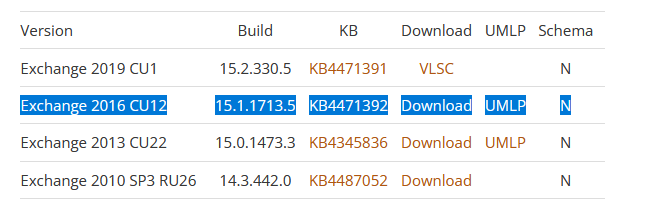






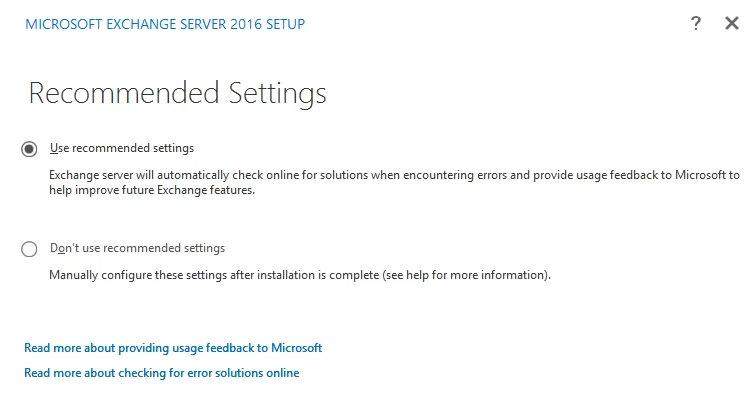
These are the steps I took and the setting I configured to set up the Active Directory, which the exchange server requires to work properly.

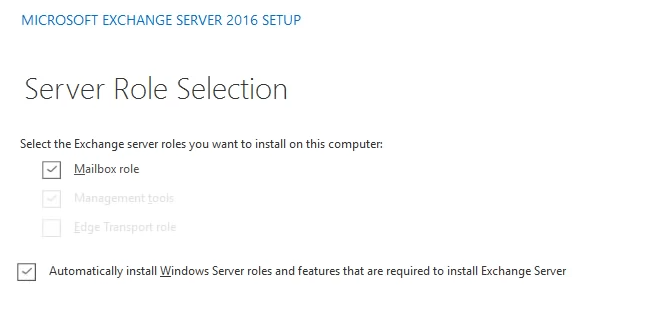
The next step is downloading the files for the exchange server.



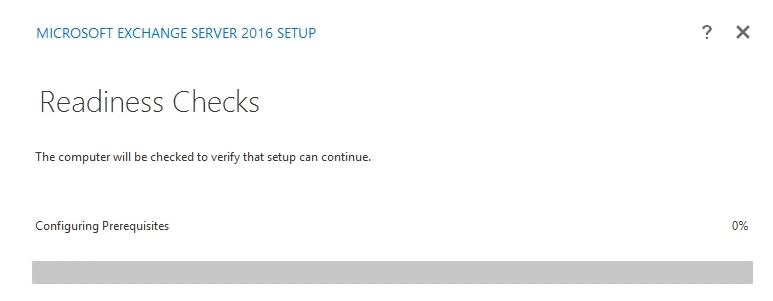
I downloaded the files on my host then transferred them onto the VM to be extracted, once they are then the set up of the exchange server can begin.

Here are the setting I configured:

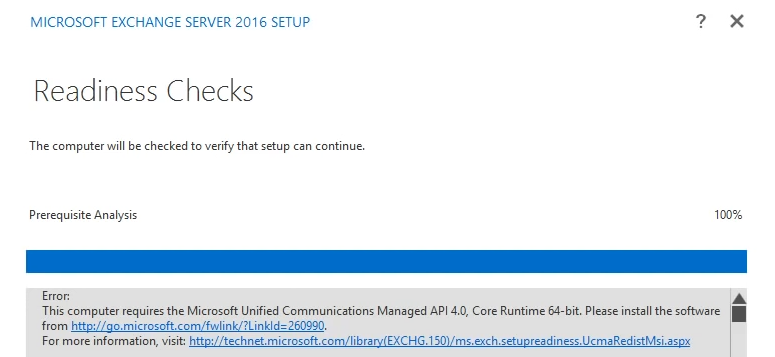




Then it does readiness checks to determine if everything is configured correctly, this can take a very long time to load.



Here is where I had our most major issue, there was missing files that needed to be downloaded, and for some reason downloading them directly onto the VM did not work properly, after many many many different fixes I finally figured out if I download specific files onto my host machine then transfer them onto the VM I could get it to work.

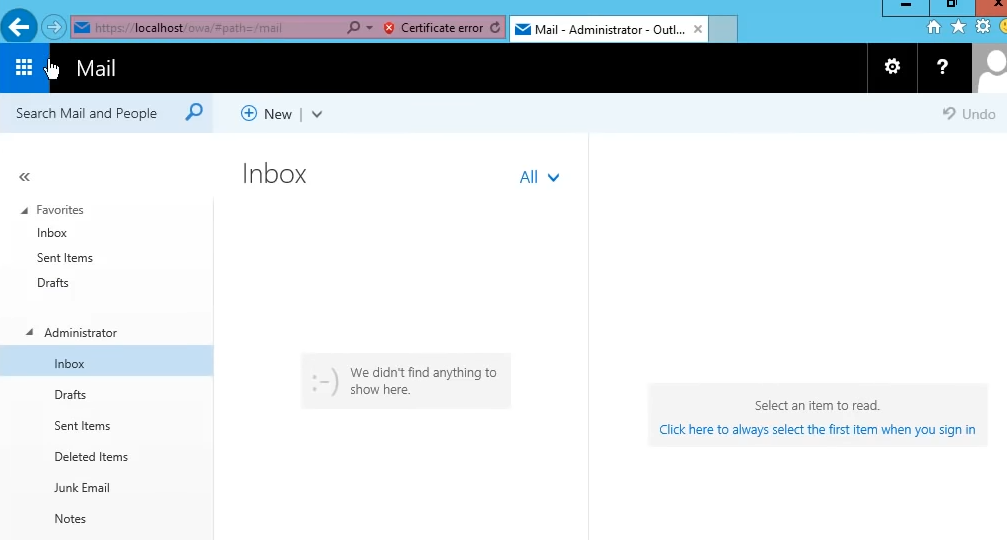


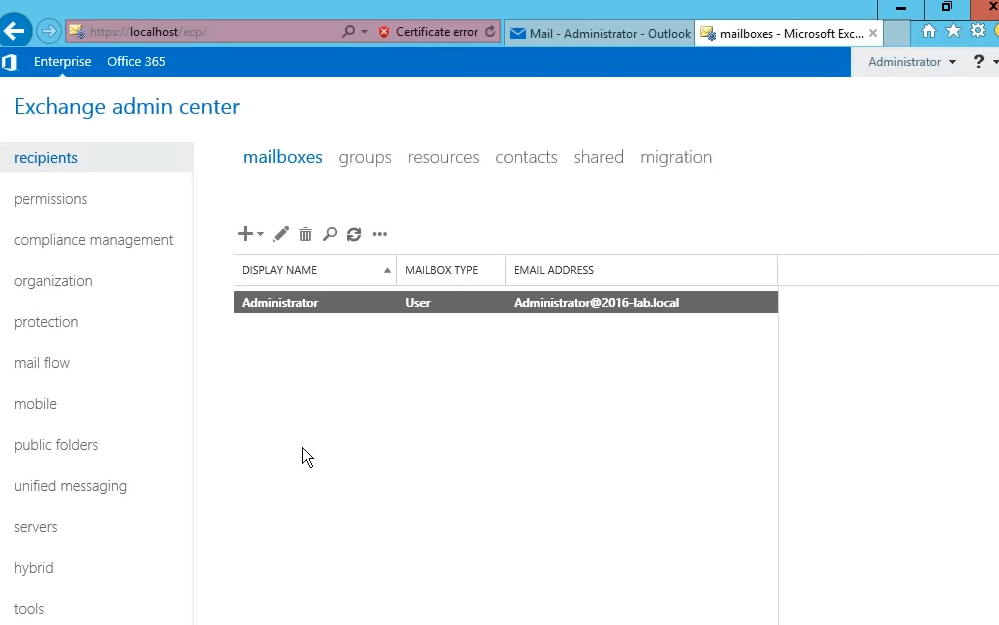
Finally after much trial and error I got the prerequisites install and then the server was ready to be configured

And we wait, for a very long (hours long) time for the server setup to finish.



And finally, after all that, the exchange server is set up, we can now access the email service and admin control panel.

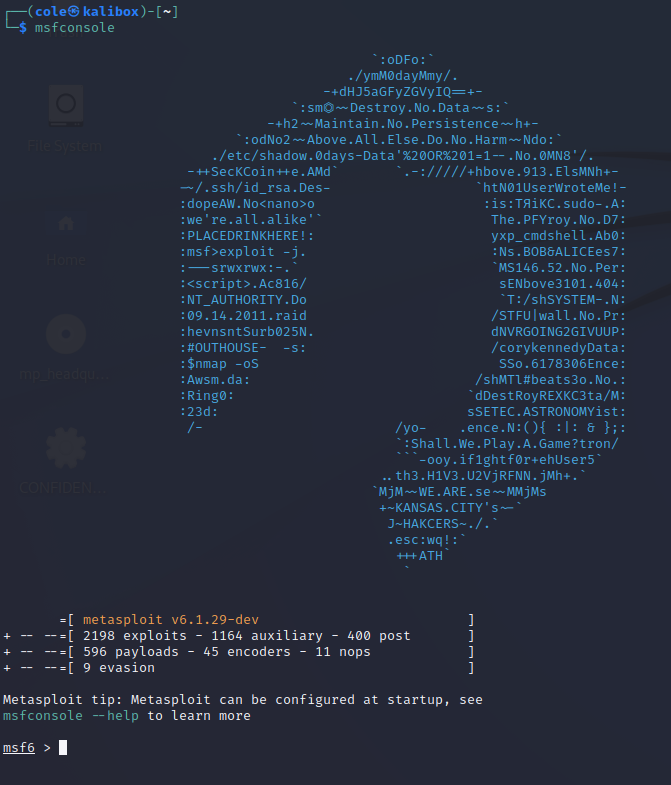




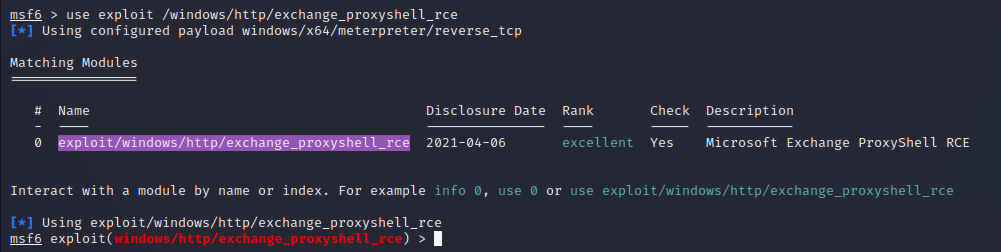
**The Attack:**

After the set up of the server, the attack is really straight forward.

First, we open the Metasploit console

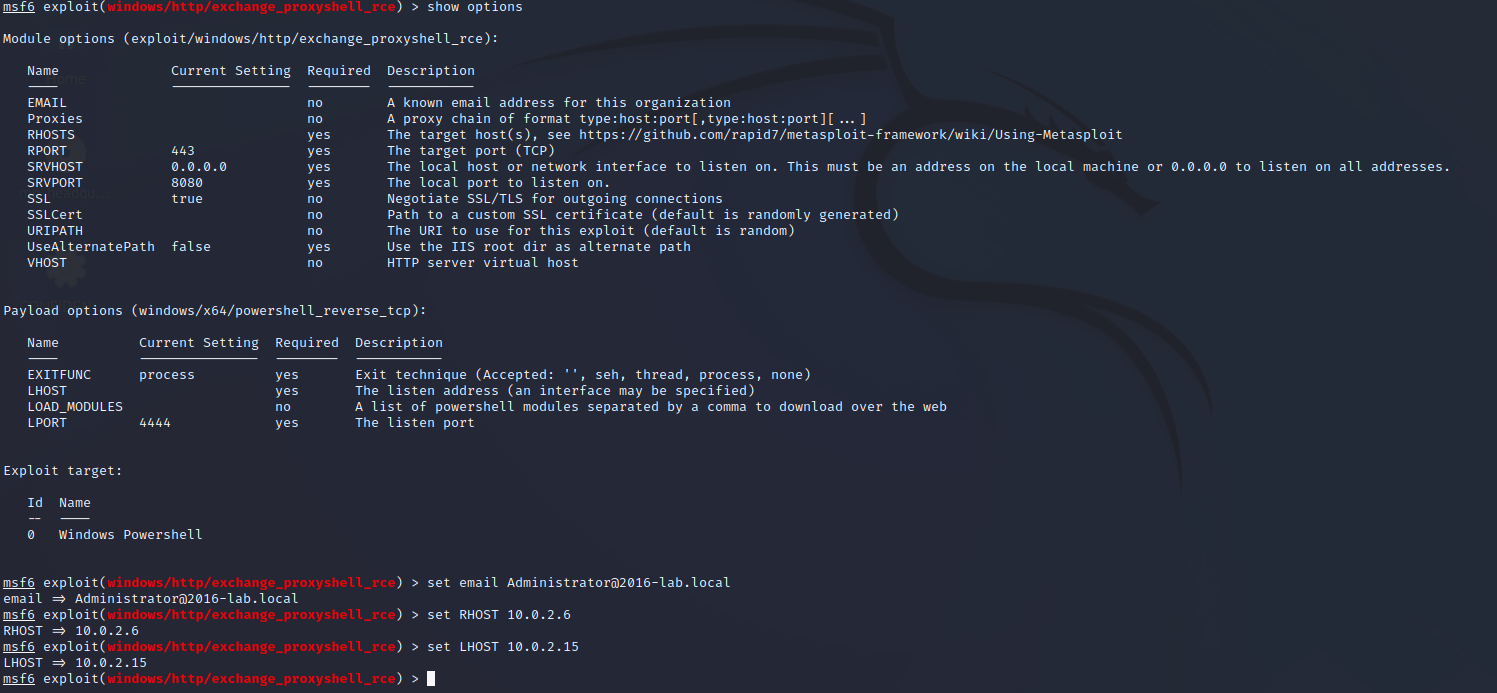


Then, we select the right exploit and payload to implement





Then we configure the options



And we are good to go! Simply type the command exploit and a PowerShell session opens on the victim’s machine, ready for further malicious exploits depending on the will of the attacker. This exploit was scary easy to do, but luckily the vulnerability has been patched and this no longer works on up to date exchange servers.