|  |  |
| --- | --- |
| 1. Open your Azure VM and open Hyper-V 2. Start both your Server and Workstation 3. Long into your Workstation as Administrator |  |
| 1. Open File Explorer |  |
| 1. In the search bar enter two slashes, your sever name, another slash, then NETLOGON 2. Then hit enter |  |
| 1. This is what it should look like 2. If yours does not have the chrome.msi it is ok |  |
| 1. Right click and add a new text document |  |
| 1. Call that document HoneyPot |  |
| 1. Now open the Group Policy Manager |  |
| 1. Right click on your domain name 2. Select the first option to create a GPO |  |
| 1. Call the new GPO HoneyPot 2. Click ok |  |
| 1. Right click the new GPO and click Edit |  |
| 1. Go under Policies, Windows Settings, Security Settings, Local Policies, Audit Polies 2. Your screen should look like this |  |
| 1. Now double click the first audit option and this screen should appear |  |
| 1. Check off every box and click apply |  |
| 1. Now go to the second audit option |  |
| 1. Click every box then click apply and ok |  |
| 1. Now to the third option |  |
| 1. Here click only the top two boxes 2. Then hit apply and ok |  |
| 1. Now on the forth option do all of the boxes |  |
| 1. Skip the fifth option and go to the sixth. Click only the first two boxes 2. Then apply and ok |  |
| 1. Skip the 7th option |  |
| 1. On the next option click the top two boxes 2. Then apply and ok |  |
| 1. Now go to the last option |  |
| 1. Click the top two boxes only |  |
| 1. Now go back to the HoneyPot.txt in file explorer |  |
| 1. Right click it and select properties |  |
| 1. Go to the security tab and click advanced |  |
| 1. Go to the auditing tab and click add |  |
| 1. Up top click Select a Prompt |  |
| 1. In the bottom of the pop up, type in Everyone 2. Then hit ok |  |
| 1. Now on the right middle portion click Show Advanced Permissions |  |
| 1. Make sure your only have the first 4 boxes on the left side checked off |  |
| 1. Now go to your workstation and log in as a user who is not in IT |  |
| 1. Make sure the desktop pops up |  |
| 1. Now head back to the Server and search for the event viewer |  |
| 1. In the Event Viewer go into the windows logs |  |
| 1. All of the audit setting will be in here in different sections (the one shown in is the login one) |  |