Email Alerts with Windows PowerShell

The automated email alerts are implemented in order to notify authorized administrators of any errors or faults that could have occured. This enables the admins to take quick actions to resolve the issue that has been alerted. The following sections will go into details about the details of the Windows PowerShell scripts and how it functions.

vSphere Email Alert Script

The vSphere Email Alert Script is an automated process that checks on a daily basis whether or not the vCenter connectivity is up or down. The following will describe the script in great detail.



The figure above is the entire vSphere email alert script. It is located in one of the workstations that is executed on daily basis automatically. The purpose of this us to have the alert separate from the vSphere in order for it to execute independently from the power status of the vSphere.

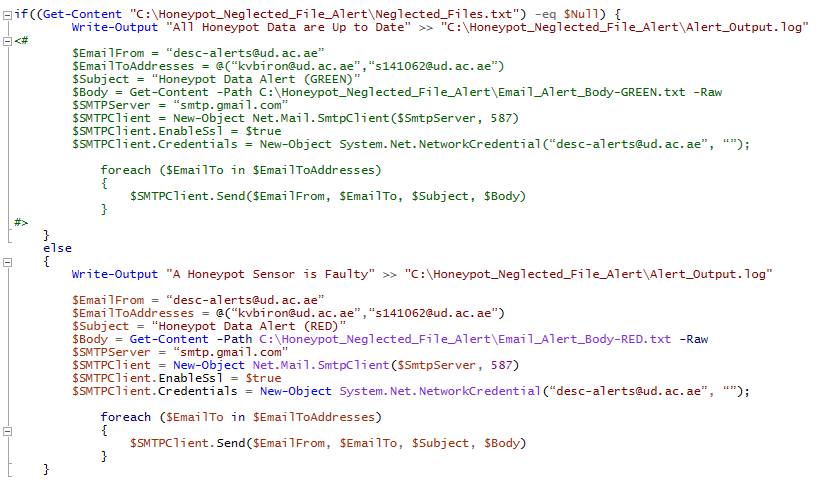
As shown above, the script starts with a set of “Write-Output” commands to log the start of the script in a log file. The main purpose of this is to enable ease of troubleshooting when an error occurs. The script then proceeds to an “IF” statement to test the reachablility of the the vCenter private IP address of 192.168.2.18. The “IF” statement will then go into one out of two options. If the connectivity test was successful, the script will only print “vSphere is REACHABLE” to the log and no emails will be sent for normal conditions as it will just bombard the administrators email inbox. On the otherhand, if the “IF” statement were not able to detect a successful connectivity to the vCenter, it will go to a code segment that will send an email alert. This command segment will send the “vSphere is UNREACHABLE” to the log file and then proceed to create variables needed to send the email alert message.

Unsynchronized Sensor Alert

The Unsynchronized Sensor Alert is an automated process that checks on a daily basis whether or not the there are any sensors that are not synchorized. If a sensor is not synchronized with the rest that could mean that the sensor has been shut down, frozen, or there are internal issues that cause the automated data synchronization from functioning as intended. The following will describe the script in great detail. One side note is that the following section will describe the Honeypot process. The Darknet process need not be explain as they have a similar process.



As shown in the figure above, this alert script start with the standard logging command set. A function called “Get-NeglectedFiles” is then created which will be utilized to check for any unsychronized CSV files. The function is then called upon to be executed on a folder where all CSV data are updated on a real time basis.



The next segment of the script is the “IF” statement. If all CSV files are up to date in the date and time of this scripts execution, only a “All Honeypot Data are Up to Date” message will be logged but no emails are sent. However, if there are any CSV files that are detected to be outdated an alert message will be sent out to the administrator.