Metasponse v 1.5.3.1 SOP

Create and Run a New Job

- From any Metasponse page, click the + New Job navbar item
- Give the job a name
  - Typically during execution, this name should be given to you by a crew lead and refer to a date, set of collectors, and target list
  - For example, if today is June 21st, and you are running all collectors against a target list labeled “W1”, your job would be titled “621.all.w1”
  - Consistent job names enables quick lookup of job results within Kibana and will help validate collection results
- Under Collectors, select the collectors as indicated by your crew commander
  - For example, if you were running all collectors against a set of Windows targets, you would select all collectors labeled “cpt_[collector type]_windows”, HashFilesystem, and RAIR
  - Do not combine two OS types in one job or template (e.g. cpt_system_windows and cpt_system_solaris cannot run at the same time)
- Under Transports, select the transports appropriate for the systems which your crew commander has assigned you to target
  - For Windows systems, select SMB and WMI
  - For Unix systems (including RedHat and Solaris), select SSH
- Under Analyzers, select the ElasticSearch Analyzer
- Under the Analysis section, enter the ElasticSearch Server’s URL/IP address

- Under Authentication
  - If using SMB and WMI, populate the Domain, Password, and Username fields, ensuring the Privilege Escalation field is set to “On”.
  - If using SSH, populate the SSH SU User (likely root), SU Password(likely root password), Unix username, and Unix Password fields, ensuring the Privilege Escalation is set to “On” and the SU Enabled box is checked.
- Under Deployment
  - Populate the Target Addresses field with the targe Ips assigned from your crew commander (do not use hostnames)
- Under Logging
  - Ensure Logging level is set to “error”
  - Ensure Plugin Debug box is checked

- Under Pickup
  - Ensure the Maximum Pickup File field is set >= 3 Gigabytes
  - Ensure the Pickup Delay is set to >=600 Minutes
  - Ensure the Pickup Timeout is set to >= 20 Minutes
- If the server has been configured correctly according to this guide, all other default values should be left as they are
- To run the job
  - Ensure target list is accurate using a two-person integrity check
  - After receiving approval from crew commander, click the schedule button to the start job.

Job Pickup

- Gathering collected information
  - Once determined that no further scripts are being executed on a target using the methods mentioned above and approval has been given by the crew commander, click ⭡ Begin Pickup from the job page
  - Pickup is complete when the ✎✎ Job Data panel containing the ▤▤ Analysis button appears
  - Click ▤▤ Analysis to view the results in the raw JSON format under the Miscellaneous panel
  - Pickup may take a long time depending on the number of remote systems and the collectors run. For jobs with particularly large amounts of data, information on the job page regarding pickup may seem to get stuck. In many of these cases, all data has been retrieved from the remote host, but the pickup completion is awaiting ElasticSearch ingestion. To verify:
    - Use Get-TerrainStatus to verify no files remain on the target systems as described in the above section
    - Open the Discover tab in Kibana and navigate to the ms-* index
      - Click "Add a filter +" at the top, with "job_name" as the field, "is" as the operator, and [job name] for the value
      - Take note of the hit count listed at the top of the page, and refresh a couple of times. If the number is growing, pickup is still waiting on ElasticSearch ingestion