MSTICPy and Jupyter Notebooks for Repeatable Threat Hunting

TEAM ASSA

SAI GANESH SENTHIVEL ALBERT LIN SKYLAR GAO AAROMAL SUJITH

Mystic MSTICPy

- **THREAT HUNTING**

  Proactively searching for threats that cannot otherwise be located with passive threat detection methods

- **REPEATABLE**

  1. One tool to hunt for all kinds of threats.
  2. Extensible modular customizable

- **SOLUTION: MSTICPY IN JUPYTER NOTEBOOKS**

  1. Connect to various network monitoring interfaces
  2. Write own queries
  3. Advantage - Pandas Dataframes

The Lab

ADDON

1. Pandas
2. Jupyter
3. Python

STAGE 1: EXPLORE

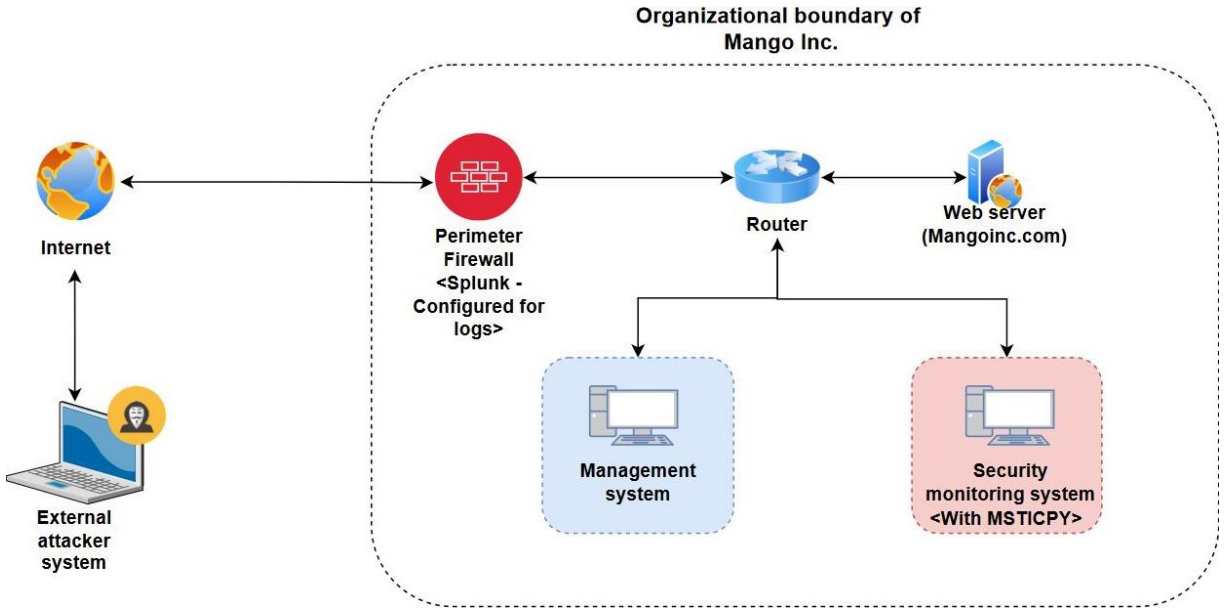
Explore and utilize MSTICPY

STAGE 2: EXPLOIT

Multi-stage real world simulated exploit on Mango Inc.

STAGE 3: TRIAL BY FIRE

Put your MSTICPY and ADDON knowledge to test



Stage 1: Explore

1. LAUNCH AND EXPLORE JUPYTER
2. INITIALIZE MSTICPY
3. QUERY AND IMPORT SAMPLE DATA
4. ANALYZE (BASE64 DECODING AND IOC EXTRACTION)
5. VISUALIZE DATA (FOLIUMMAP, ENTITYGRAPH, PROCESS TREE AND TIMELINE)

Stage 2: Exploit

1. BRUTEFORCE WEBSERVER
2. REVERSED FILE EXTRACTION (CVE-2016-4806)
3. COMPROMISE WEB SERVER (SSH). INTERNAL FTP INTO MGMT
4. STEAL CUSTOMER DATA FROM MGMT

Stage 3: Trial by fire

1. SETUP SPLUNK -> MSTICPY
2. LEARN BASICS OF INTERACTING WITH SPLUNK DATA
3. UTILIZE YOUR NEWFOUND KNOWLEDGE TO ANALYZE THE ATTACK

Conclusion

- ✔ **ALLOW ONLY ESSENTIAL SERVICES THROUGH THE FIREWALL**
- ✔ **ALWAYS PATCH ALL SERVICES**

  Update Web2py to 2.14.6
- ✔ **MSTICPY**

  The more you know python and pandas the more you can customize it.
- ✖ **MSTICPY REQUIRES INTERNET**

  We have made extensive modifications to the library in multiple places to support for this lab