Team: Cyber Defense

Assignment Task week 4 on Rastrea2r for Tutelr Infinity Internship and CSCOI Community

Objective: The objective of this assignment is to familiarize interns with the Rastrea2r tool and its capabilities. The interns will learn how to use Rastrea2r for incident response and hunting for Indicators of Compromise (IOCs) across thousands of endpoints.

Task 1: Installation and Setup

1.1. Install Rastrea2r on a virtual machine running Linux OS (Ubuntu preferred).

1.2. Configure the tool with a set of basic rules and indicators of compromise (IOCs) to start with.

Task 2: Basic Usage

2.1. Run a scan on a test system to identify IOCs.

2.2. Analyze the results of the scan and interpret the findings.

2.3. Generate a report on the findings and share it with the mentor.

Task 3: Advanced Usage

3.1. Develop custom rules and IOCs to extend the capability of the tool.

3.2. Run a scan with the custom rules and IOCs.

3.3. Analyze the results of the scan and interpret the findings.

3.4. Generate a report on the findings and share it with the mentor.

Task 4: Integration with Other Tools

4.1. Integrate Rastrea2r with another incident response tool (such as TheHive or MISP) to enable automated response to incidents.

4.2. Demonstrate the integration by running a test scenario and generating a report on the findings.

Task 5: Write a Blog Post

5.1. Write a blog post on your experience with Rastrea2r, including details on installation and setup, usage, and integration with other tools.

5.2. Share the blog post with the mentor and the CSCOI community.

Deliverables:

- A report on the findings from tasks 2 and 3.
- A report on the integration of Rastrea2r with another incident response tool in task 4.
- A blog post on the experience with Rastrea2r in task 5.
- Note: The interns are expected to complete the tasks in a timely and professional manner. The mentor will be available for guidance and support throughout the assignment.

Submission

Click here to Submit your Week 4 Assignment

Guide: Sriram K

Due on: 15th April 2023

Assessment

1. What is Rastrea2r?
    A. A multi-platform open-source tool
    B. A closed-source tool for incident response.
    C. A tool for tracking social media activity
    D. A tool for tracking online advertising campaigns

2. What does Rastrea2r allow incident responders and SOC analysts to do?
    A. Triage suspect systems
    B. Monitor employee productivity
    C. Conduct background checks on individuals
    D. Encrypt sensitive data

3. What is an IOC in the context of Rastrea2r?
    A. An incident of compromise
    B. An indicator of compliance
    C. An instruction for using the tool
    D. A report generated by the tool

4. How long does it take Rastrea2r to search thousands of endpoints for IOCs?
    A. Days
    B. Hours
    C. Minutes
    D. Seconds

5. What platforms does Rastrea2r support?
    A. Windows only
    B. macOS only
    C. Linux only
    D. Multiple platforms

6. What types of IOCs can Rastrea2r search for?
    A. Malware
    B. IP addresses
    C. Domains
    D. All of the above

7. Does Rastrea2r require installation on each endpoint?
    A. Yes
    B. No

8. Can Rastrea2r be used for threat hunting?
    A. Yes
    B. No

9. What is the pronunciation of Rastrea2r?
    A. "Rastreeter"
    B. "Rastreador"
    C. "Rastrar"
    D. "Rastrador"

10. Is Rastrea2r a free or paid tool?
    A. Free
    B. Paid
    C. Both free and paid versions are available
    D. It depends on the number of endpoints being searched.

Submission

Click here to Submit your Week 4 Assignment