Security Operations Center SOC in a box

Creating an economic SOC (Security Operations Center) in a box solution by integrating the ELK Stack, TheHive, MISP, and related components is a great idea. Here’s a detailed step-by-step guide for installing and configuring these tools on an Ubuntu server. This guide assumes you’re using Ubuntu 22.04 LTS or a later version.

**Prerequisites**

1. **Ubuntu Server**: Make sure you have a fresh installation of Ubuntu Server 22.04 or later.
2. **Root or Sudo Privileges**: Ensure you have root or sudo privileges for installing software and making system changes.
3. **Network Configuration**: Ensure your server has a static IP address.

**1. System Update and Basic Setup**

Start by updating your system and installing basic dependencies:

sudo apt update

sudo apt upgrade -y

sudo apt install -y curl wget gnupg software-properties-common

**2. Install the ELK Stack**

**2.1 Install Java (for Elasticsearch)**

Elasticsearch requires Java. You can install OpenJDK 11:

sudo apt install -y openjdk-11-jdk

**2.2 Install Elasticsearch**

Add the Elastic APT repository and install Elasticsearch:

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

sudo sh -c 'echo "deb https://artifacts.elastic.co/packages/8.x/apt stable main" > /etc/apt/sources.list.d/elastic-8.x.list'

sudo apt update

sudo apt install -y elasticsearch

Configure Elasticsearch to start on boot and start the service:

sudo systemctl enable elasticsearch

sudo systemctl start elasticsearch

Verify the installation:

curl -X GET "localhost:9200/"

**2.3 Install Logstash**

Add the Logstash package and install it:

sudo apt install -y logstash

Start and enable Logstash:

sudo systemctl enable logstash

sudo systemctl start logstash

**2.4 Install Kibana**

Install Kibana:

sudo apt install -y kibana

Configure Kibana by editing /etc/kibana/kibana.yml:

sudo nano /etc/kibana/kibana.yml

Set the following configuration (update with your server’s IP address):

server.host: "0.0.0.0"

elasticsearch.hosts: ["http://localhost:9200"]

Enable and start Kibana:

sudo systemctl enable kibana

sudo systemctl start kibana

Access Kibana by visiting http://<your-server-ip>:5601 in a web browser.

**2.5 Install Elastic Agent and Fleet Server**

Install Elastic Agent:

sudo apt install -y elastic-agent

*Configure Fleet Server by creating a Fleet policy and enrolling the Elastic Agent. Instructions for this are available in the Kibana UI under the Fleet section. In this part you may require to create several policies and link it to existing main policy.*

**3. Install TheHive**

**3.1 Install Dependencies**

TheHive requires MongoDB and OpenJDK 11:

sudo apt install -y mongodb

sudo apt install -y openjdk-11-jdk

**3.2 Install TheHive**

Download and install TheHive:

wget https://dl.bintray.com/thehive-project/debian/thehive\_4.1.1-1\_amd64.deb

sudo dpkg -i thehive\_4.1.1-1\_amd64.deb

sudo apt-get install -f

Configure TheHive by editing /etc/thehive/application.conf and setting the MongoDB URL and other parameters:

sudo nano /etc/thehive/application.conf

Start TheHive:

sudo systemctl enable thehive

sudo systemctl start thehive

Access TheHive by visiting http://<your-server-ip>:9000 in a web browser.

**4. Install MISP**

**4.1 Install Dependencies**

MISP requires Apache, MySQL, and PHP:

sudo apt install -y apache2 mysql-server php php-mysql libapache2-mod-php php-xml php-mbstring

**4.2 Install MISP**

Clone the MISP repository and set it up:

cd /var/www

sudo git clone https://github.com/MISP/MISP.git misp

cd misp

sudo git submodule update --init –recursive

Set permissions:

sudo chown -R www-data:www-data /var/www/misp

sudo chmod -R 750 /var/www/misp

Configure Apache for MISP:

sudo nano /etc/apache2/sites-available/misp.conf

Add the following configuration:

<VirtualHost \*:80>

ServerAdmin admin@localhost

DocumentRoot /var/www/misp/app/webroot

ServerName <your-server-ip>

ErrorLog ${APACHE\_LOG\_DIR}/error.log

CustomLog ${APACHE\_LOG\_DIR}/access.log combined

<Directory /var/www/misp/app/webroot>

AllowOverride All

Require all granted

</Directory>

</VirtualHost>

Enable the site and restart Apache:

sudo a2ensite misp

sudo systemctl restart apache2

**4.3 Configure MISP**

Set up MISP by following the official MISP documentation for configuration. You’ll need to edit the MISP configuration files and set up the database.

**5. Integrate Components**

**5.1 Integrate TheHive with ELK**

Configure TheHive to send alerts to ElasticSearch:

1. Access TheHive’s settings.
2. Configure the integration with Elasticsearch under the "Cortex" section.

**5.2 Integrate MISP with TheHive**

Install the MISP-Cortex plugin for TheHive:

cd /opt/thehive/cortex-plugins

sudo git clone https://github.com/Cortex-Plugins/misp

sudo chown -R thehive:thehive misp

Configure TheHive to use MISP:

1. Go to the TheHive UI.
2. Navigate to the "Cortex" section and configure the MISP plugin.

**6. Final Testing and Verification**

1. **Verify Elasticsearch**: Ensure it is properly indexing and storing data.
2. **Verify Kibana**: Confirm that Kibana is visualizing logs from Logstash.
3. **Verify TheHive**: Test incident creation and integration with Elasticsearch.
4. **Verify MISP**: Ensure MISP is functioning and able to share and receive threat intelligence.

**Conclusion**

You now have a basic SOC in a box setup with ELK Stack, TheHive, and MISP running on your Ubuntu server. You can further configure and tune each component according to your specific needs. Regular updates and security practices are essential to keep your SOC effective and secure.

Automic Red Team Simulation Tutorials:

<https://attack.mitre.org/matrices/enterprise/>

<https://www.youtube.com/watch?v=_xW3fAumh1c>

<https://www.youtube.com/watch?v=-HEx-qfd54M&list=PL92eUXSF717W9TCfZzLca6DmlFXFIu8p6>

<https://www.youtube.com/watch?v=iNl_rltYmoo&list=PL92eUXSF717XLqkiCitdSZSUijwdDsM20>

<https://www.youtube.com/watch?v=O6w0oFcCAnI>

Caldera Red Team Simulation Tutorials:

<https://github.com/mitre/caldera>

<https://www.youtube.com/watch?v=EIHLXWnK1Dw>

<https://caldera.readthedocs.io/en/latest/>

**Step-by-Step Guide: Setting Up and Generating Attacks with Atomic Red Team**

**1. Prepare Your Environment**

1. **Ensure Windows Machines are Ready:**
   * Confirm that you have Windows 10/11 machines available for testing.
   * Ensure they have the latest updates and necessary security configurations.
2. **Create Virtual Machines (Optional):**
   * Using virtualization software like VMware or Hyper-V, create a snapshot of your base machine before running any tests. This allows for quick restoration.
3. **Install Required Tools:**
   * Make sure you have tools like PowerShell, Git, and any other prerequisites installed on your machines.

**2. Install and Configure Atomic Red Team**

1. **Download Atomic Red Team:**
   * Open PowerShell as Administrator.
   * Clone the Atomic Red Team repository using Git:

git clone <https://github.com/redcanaryco/atomic-red-team.git>

1. **Navigate to the Atomic Red Team Directory:**

cd atomic-red-team

1. **Install Required Modules:**
   * Atomic Red Team uses various scripts, so ensure that the necessary PowerShell modules are installed. You might need PowershellGet and PSReadline.

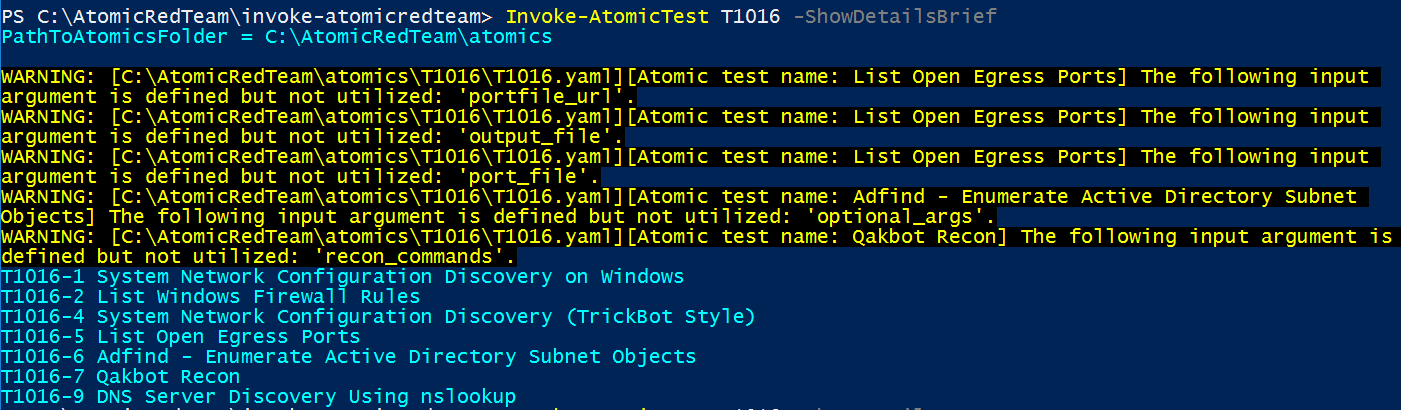
**3. Select and Run Atomic Tests**

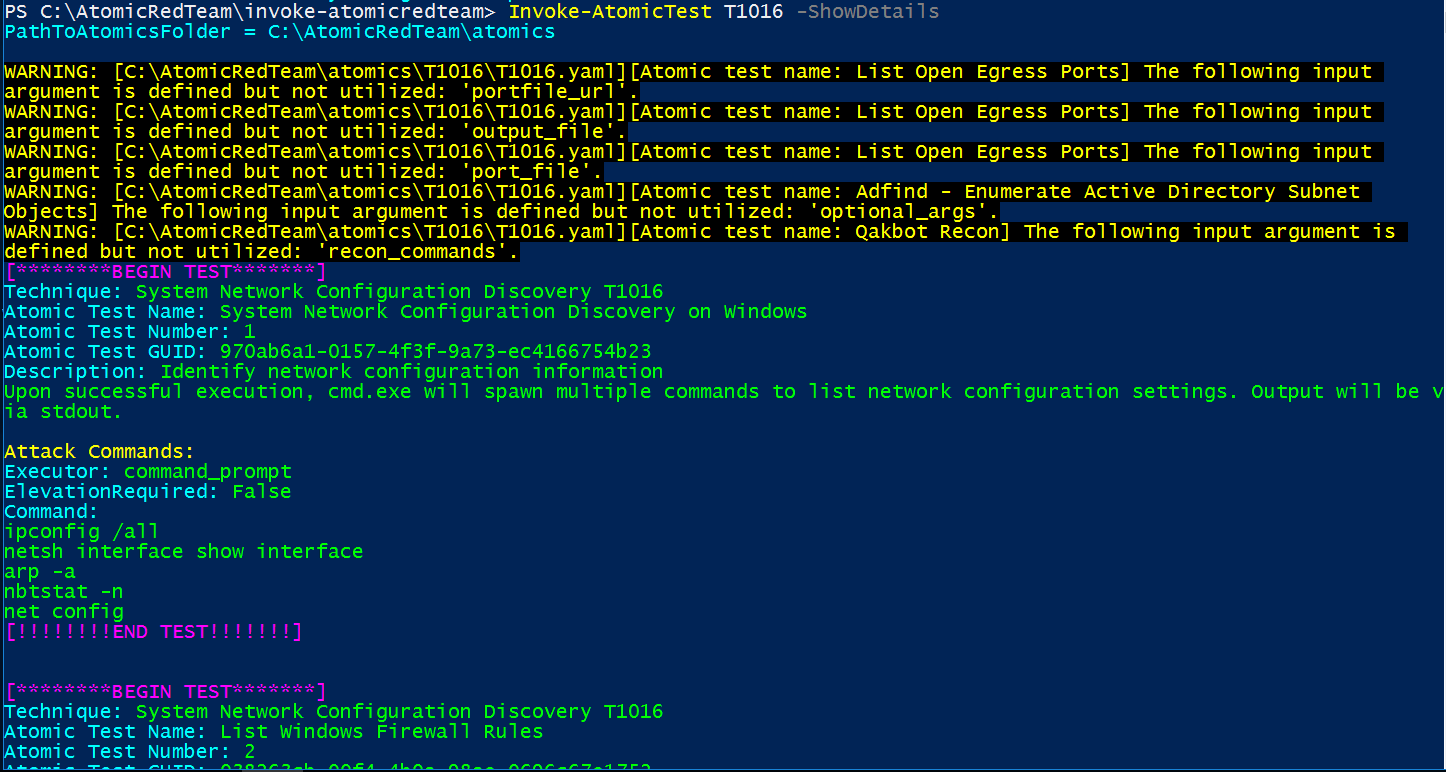
1. **Browse Atomic Red Team Tests:**
   * Go to the atomics folder in the Atomic Red Team repository:

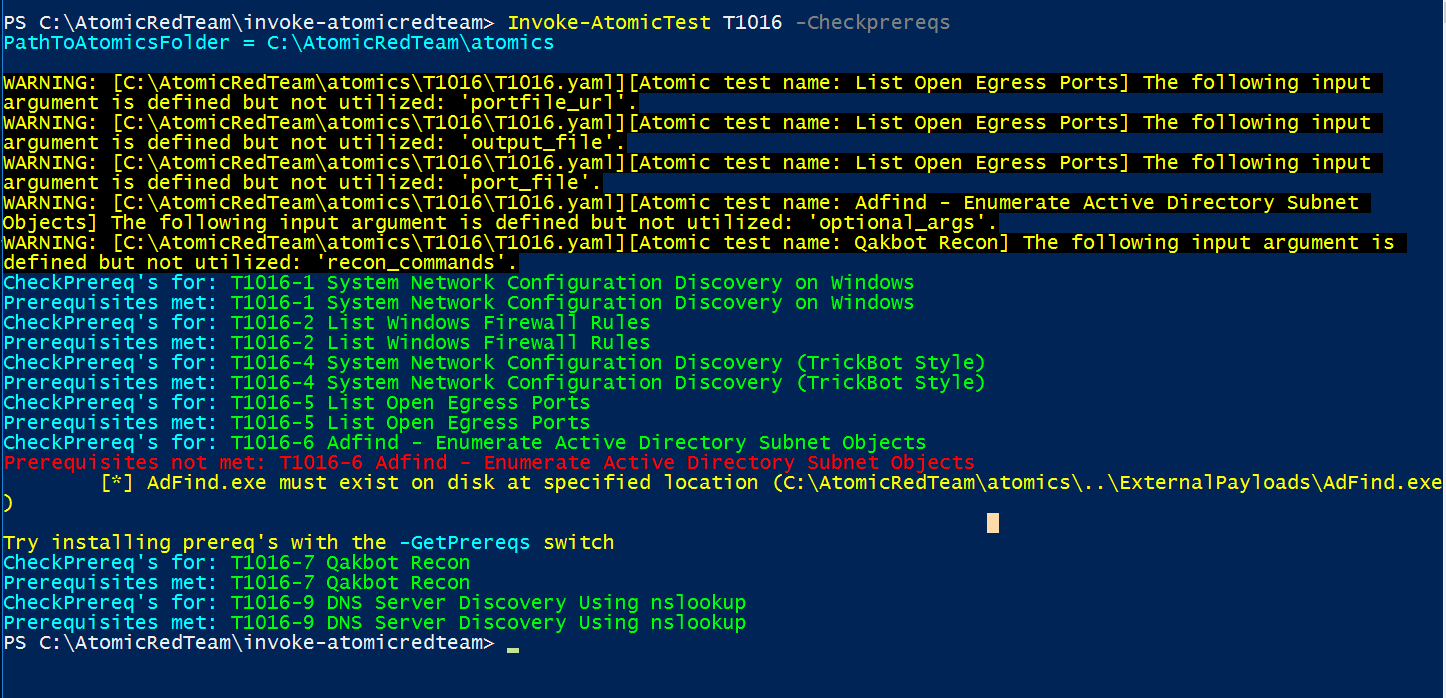
cd atomics

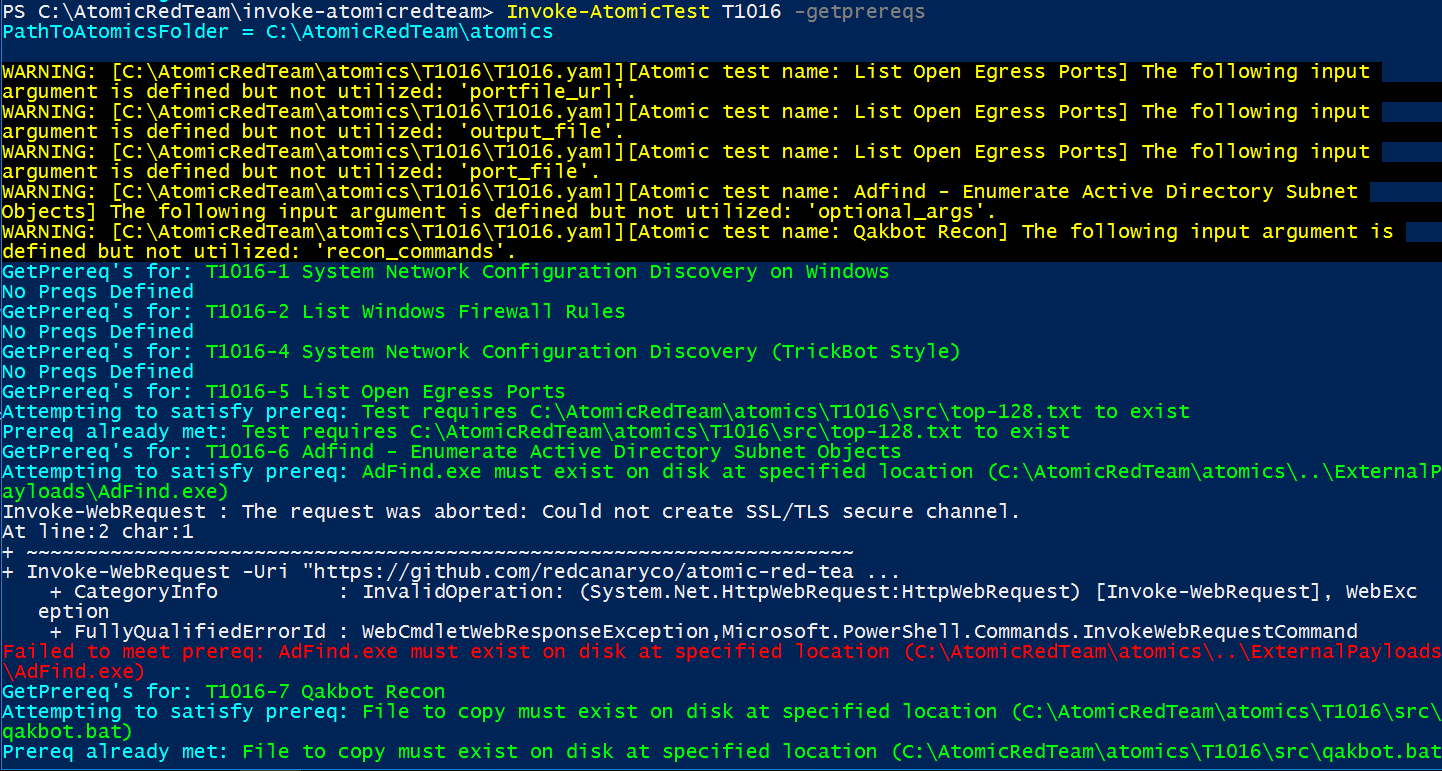
* Review the test scenarios available. Each test is categorized by MITRE ATT&CK technique.

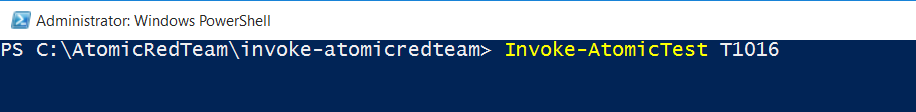


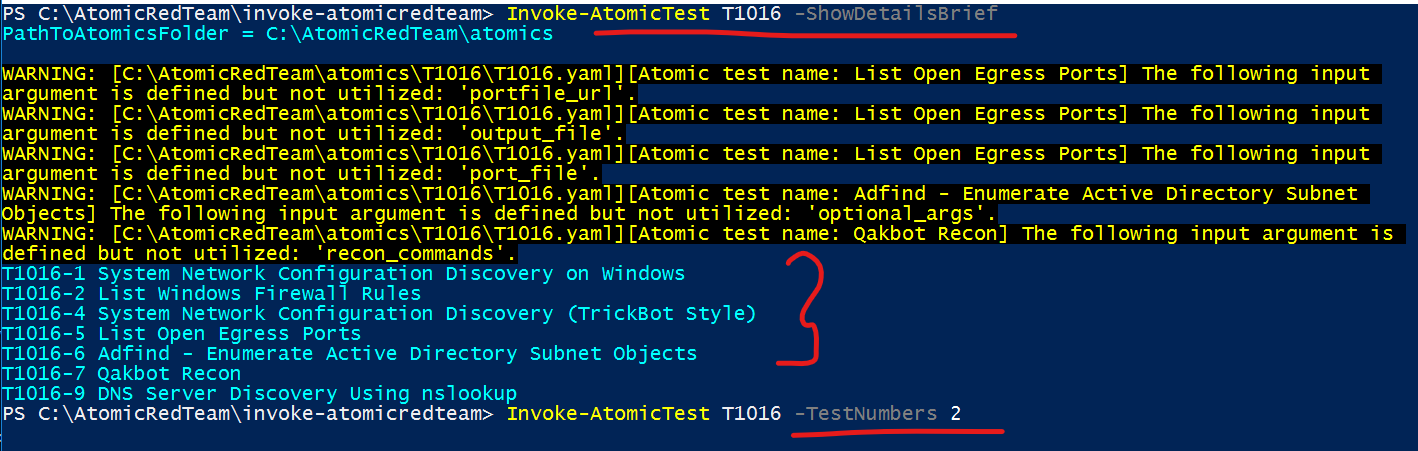


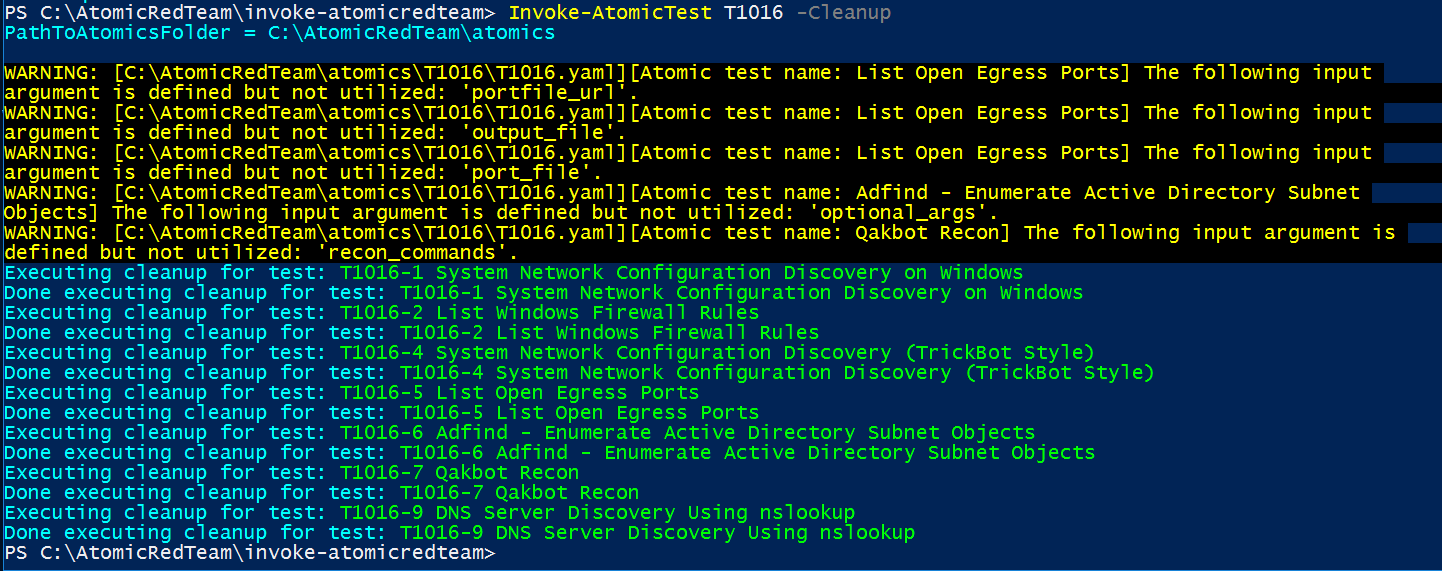












1. **Select a Test to Run:**

* Navigate to a specific technique directory. For example, to test technique T1003 (Credential Dumping):

cd T1003

**Run a Test:**

* Execute the PowerShell script for the selected test. For example:

.\T1003\_Credential\_Dumping.ps1

* + Ensure that you follow any instructions provided in the test script, such as running the script as an Administrator.

**4. Monitor and Analyze the Attacks**

1. **Enable Windows Event Logging:**
   * Ensure that Windows Event Logging is enabled to capture the attacks. You can enable auditing through Group Policy:
     + Open gpedit.msc.
     + Navigate to Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration.
     + Configure policies under Audit Policies to ensure relevant logs are captured.
2. **Observe the Attacks:**
   * Use Event Viewer (eventvwr.msc) to view logs generated by the attacks.
   * Focus on Security, Application, and System logs.
3. **Use a SIEM (Optional):**
   * If you have a Security Information and Event Management (SIEM) tool, configure it to collect and analyze logs. Examples include Splunk, ELK Stack, or Microsoft Sentinel.

**Select and Run Atomic Tests**

**Privilege Escalation**

1. **Technique T1068 (Exploitation for Client Execution):**
   * Navigate to the directory:

cd atomics/T1068

Run the test:

.\T1068\_Exploitation\_for\_Client\_Execution.ps1

1. **Technique T1203 (Exploitation for Client Execution):**

* Navigate to the directory:

cd atomics/T1203

.\T1203\_Exploitation\_for\_Client\_Execution.ps1

**Network Configuration**

1. **Technique T1021 (Remote Services):**
   * Navigate to the directory:

cd atomics/T1021

.\T1021\_Remote\_Services.ps1

1. **Technique T1071 (Application Layer Protocol):**

* Navigate to the directory:

cd atomics/T1071

.\T1071\_Application\_Layer\_Protocol.ps1

**Audit Logs**

1. **Technique T1005 (Data from Local System):**
   * Navigate to the directory:

cd atomics/T1005

.\T1005\_Data\_from\_Local\_System.ps1

**Technique T1083 (File and Directory Discovery):**

* Navigate to the directory:

cd atomics/T1083

.\T1083\_File\_and\_Directory\_Discovery.ps1

**Firewall Policy**

1. **Technique T1205 (Traffic Injection):**
   * Navigate to the directory:

cd atomics/T1205

.\T1205\_Traffic\_Injection.ps1

**Technique T1562 (Impair Defenses):**

* Navigate to the directory:

cd atomics/T1562

.\T1562\_Impair\_Defenses.ps1

**Boot Process**

1. **Technique T1542 (Pre-OS Boot):**
   * Navigate to the directory:

cd atomics/T1542

.\T1542\_Pre-OS\_Boot.ps1

**Technique T1053 (Scheduled Task/Job):**

* Navigate to the directory:

cd atomics/T1053

.\T1053\_Scheduled\_Task\_Job.ps1

**Driver Installation**

1. **Technique T1210 (Exploitation of Remote Services):**
   * Navigate to the directory:

cd atomics/T1210

.\T1210\_Exploitation\_of\_Remote\_Services.ps1

**Technique T1216 (System Information Discovery):**

* Navigate to the directory:

cd atomics/T1216

.\T1216\_System\_Information\_Discovery.ps1

**Windows Update**

1. **Technique T1059 (Command and Scripting Interpreter):**
   * Navigate to the directory:

cd atomics/T1059

.\T1059\_Command\_and\_Scripting\_Interpreter.ps1

**Technique T1087 (Account Discovery):**

* Navigate to the directory:

cd atomics/T1087

.\T1087\_Account\_Discovery.ps1

**Windows Defender Events**

1. **Technique T1040 (Network Sniffing):**
   * Navigate to the directory:

cd atomics/T1040

.\T1040\_Network\_Sniffing.ps1

**Technique T1203 (Exploitation for Client Execution):**

* Navigate to the directory:

cd atomics/T1203

.\T1203\_Exploitation\_for\_Client\_Execution.ps1

**5. Evaluate and Document**

1. **Assess Detection Capabilities:**
   * Evaluate how well your SOC analysts can identify the generated attacks by analyzing the collected logs.
   * Document the effectiveness of their responses and detection capabilities.
2. **Review and Improve:**
   * Discuss the findings with your SOC team.
   * Identify any gaps in detection or response.
   * Make adjustments to your security policies or monitoring tools based on the results.

**6. Reset and Cleanup**

1. **Restore Machines:**
   * If using virtual machines, revert to the pre-snapshot state.
   * For physical machines, consider running a cleanup script or manually restoring the system to its original state.
2. **Remove Atomic Red Team Artifacts:**
   * Delete any files or scripts left behind from the Atomic Red Team tests.

**Additional Tips**

* **Documentation:** Make sure to provide detailed instructions and any required scripts in your lab documentation.
* **Safety:** Ensure that all tests are conducted in a controlled environment to avoid unintended disruptions.
* **Updates:** Regularly update Atomic Red Team and related tools to incorporate new tests and techniques.

Feel free to customize the guide according to the specific needs and setup of your SOC environment.