Microsoft 365 Defender simulation

Atomic Red Team – Linux Techniques Simulation

November 2021

Summary

This Linux simulation is a compilation of tests provided by Atomic Red Team™, an open-source library of simple, focused tests designed to emulate adversary techniques. These atomic tests allow security teams to seamlessly run a collection of safe tests for prevalent malicious behaviors on Linux, and validate their defense against these techniques.

The simulation consists of the following steps:

Persistence	Local account creation
Discovery	Browser bookmark discovery
Discovery	File and directory discovery
Discovery	System information discovery
Defense Evasion	File obfuscation

Running the simulation

> Note: We recommend running this simulation in a testing environment such as the Evaluation lab. You can also run the simulation on any other device of your choice.

To run the simulation in the evaluation lab, follow these steps:

1. Navigate to **Evaluation & tutorials** > **Evaluation lab**.
2. Go to the **Devices** tab and click **Add Device**. Follow the wizard to create a Linux device. Save the provided credentials.
3. Once the device is ready, click the Actions button (⋮), then click **Connect**, and connect to the device using your preferred SSH client.
4. Download the simulation script, unzip it, copy it to the device and run it by executing:
   ```
   chmod +x linux_simulation.sh
   sudo ./linux_simulation.sh
   ```

Simulation steps

Local account creation MITRE T1136.001

This test safely creates a standard, but expired, user account on the endpoint, and adds the user to the root group. Then, the user is removed.

> Investigation tip: Search for an alert named "**Creation of suspicious user account**".

Browser bookmark discovery MITRE T1217

This test, designed around the Firefox browser on Linux desktops, finds and creates a copy of the bookmarks available to it; then creates, writes, and deletes the file.

> Investigation tip: Look for alerts such as "**Suspicious browser manipulations or access**" and "**Suspicious file and directory discovery"**.

File and directory discovery MITRE T1083

In the above test, standard paths and applications are used to query the user's home directory for PDF files and other information.

> Investigation tip: Search for an alert such as "**Enumeration of files with sensitive data**".

System information discovery MITRE T1082

This test runs a few commands, such as `uname`, `uptime` and others, to list OS information about the device.

> Investigation tips: Look for an alert named "**Suspicious system information discovery**".

File obfuscation MITRE T1027

This test creates a base64-encoded data file and decodes it into an executable shell script. Then, the script is executed.

> Investigation tips: Search for alerts named "**Suspicious process collected data from local system**" and "**Executable permission added to file or directory**".

About Atomic Red Team

Created by Red Canary, Atomic Red Team™ is an open-source library of tests that security teams can use to simulate adversarial activity in their environments.

Atomic tests are simple. Each test is mapped to exactly one MITRE ATT&CK® technique or sub-technique, so it's comparatively easy to develop a focused testing strategy. Most of the time, you don't have to install any software to run an atomic test, and many tests come with easy-to-use configuration and cleanup commands.

We originally created Atomic Red Team to test our own detection coverage. We found the usual testing method—executing real malware samples—to be cumbersome, potentially risky, and not representative of real-world adversary behaviors. We began work on a suite of tests mapped to MITRE ATT&CK. Atomic Red Team was released to the public in 2017.

To learn more, dive into the GitHub repo, and join our open Slack channel to connect with the maintainers and other contributors.