SIMSPACE

Cyber Cup Competition

Rules of Engagement

February 27, 2025

Range Environment Basics

Your range is a virtualized environment built to accurately simulate basic IT infrastructure, users, and network traffic. It has emulated users who conduct typical user actions, such as browsing the web, opening emails and attachments, working on various files, and clicking links. On this range, these actions are automated for simulated users, but these actions themselves are not malicious. They can, however, through phishing and other attacks, be exploited in the same way that users are exploited in most environments. The sections below outline the expectations and out-of-bounds items that are required to control and maintain the range. Do not "fight the range," if something is listed in the Out-of-Bounds List, it is not malicious and will not be exploited by the Threat “Red” Team, as is required for stable range operations.

Range Familiarization

1. Finish reading this document to understand the expectations and rules regarding the range.
2. Log into the SimSpace Portal and Mattermost.
3. Within the SimSpace Portal, navigate to your team’s Live Action Event.
    a. This will place you in the ***Event Lobby***.
4. Within the event, navigate to the ***Event Documents*** tab on the left to download useful documents related to your event.
5. Within the event, navigate to the ***Virtual Machines*** tab of the Network section on the left.
6. Open the console and log into your assigned VM.
    a. The document with suggested assignments can be found in the ***Documents*** tab of the event.
    b. Credentials can be found in the ***VM Description*** column.
7. Also in the ***Network*** section, the ***Network Map*** tab is where you can reference the network diagram for more details about your virtual network.
8. Proceed to enumerate, baseline, and scan to gain a more comprehensive understanding of your network.

Defender Challenge Expectation

Defender “Blue” Team

Your goal is to defend your network through detection and reporting of IoCs and artifacts. **Report what you see in detail such as processes, ports, hosts, files, paths, DLLs, etc.**

The Control Cell may intervene if we determine that you are focusing on an artifact-of-simulation rather than a real occurrence, or "fighting the range" itself, rather than the scenario. Ultimately, we want to ensure you have the maximum opportunity to learn and focus on detecting the real adversary tactics presented in the attacks. Standard baselining and network analysis strategies will help you achieve this focus. Try to connect anomalous network traffic you detect to the hosts and processes generating that traffic; and determine both network and host indicators of compromise.

It is important to note the out-of-bounds items listed below so they do not become distractions as you attempt to monitor and defend your network.

Out-of-Bounds List

The following items related to range control and range support are out-of-bounds for both the Threat and Defender Teams.

- 10.10.0.0/16 is the Range Control network. This network is used to administer the range and is only available to Control Cell.
  - The Threat Team will not use this network. Do not block access to this network. Do not create any firewall rulesets other than allow any to any for this IP range.
- Default SimSpace accounts are out-of-bounds and will not be used by the Threat Team.

The following processes are part of range support and should not be the focus of forensics efforts. The Threat Team will not use or inject into these processes:

- Puppet
  - Software or files located in **C:\ProgramData\PuppetLabs**
  - Software or files located in **C:\ProgramData\Puppet**
  - Software or files located in **C:\Program Files\Puppet Labs**
  - Software or files located in **C:\ProgramData\staging**
  - Ruby
  - Choria
- User Emulation
  - Software or files located in **C:\Program Files (x86)\Simspace**
  - java.exe listening/communicating on ports 49999, 49998, 5762, 15672, & 27017

    - amqp listening on port 5672
- Other
    - **systeminit.exe** and all related files to this binary

If you are unsure about an artifact you see in the range not listed above, reach out to the control cell for verification.

Other Range Rules

- **We do not allow export of files, data, or hashes from the range.**
  Submit questions, hashes, and information about suspected malware to the Control Cell through your reports.

- **We do allow tools to be added to the range.**
  Range support is always willing to accommodate requests if possible. Most requests can be completed quickly, depending on the size and type of files. Please submit a support ticket with your request.