Carnegie Mellon University
Software Engineering Institute

GreyBox

Emulate the Internet for Offline Cybersecurity Training

YOUR ORGANIZATION, LIKE MOST, NEEDS A STRONG CYBERSECURITY WORKFORCE, which means you need the training to support it. However, training your cybersecurity staff on your organization's live networks can put those networks and your data at risk.

With effective cybersecurity training, students perceive that they are actually connected to the real Internet and are dealing with real-world problems. Your challenge is to produce such a training environment without the risks that working on live systems presents.

We at the Software Engineering Institute recommend that you use training exercises and scenarios in an emulated training environment that is disconnected from real data and live networks. Having an isolated environment eliminates the risk of exploits and malware escaping and causing damage.

Internet in a Box

GreyBox is an open source emulation tool that provides the illusion to your students that they are connected to the Internet.

With GreyBox, students can access what they think are thousands of websites, and the GreyBox instance can emulate any DNS you need for your cybersecurity training. GreyBox includes dozens of backbone routers that represent major carriers and ISPs, all running in containers on the same instance. To support your training scenario, GreyBox can also add clones of public email providers with live accounts.

GreyBox Under the Hood

You can use this single-host tool on a physical or virtual machine (VM) host. Relying on TopGen, an application service emulator, and CORE, a container-based network simulator, GreyBox provides an elaborate network topology configuration that can be used to create a realistic training environment.

More features are coming soon, such as a WHOIS service and a traffic generator to make the emulated Internet come alive.

Get GreyBox Today

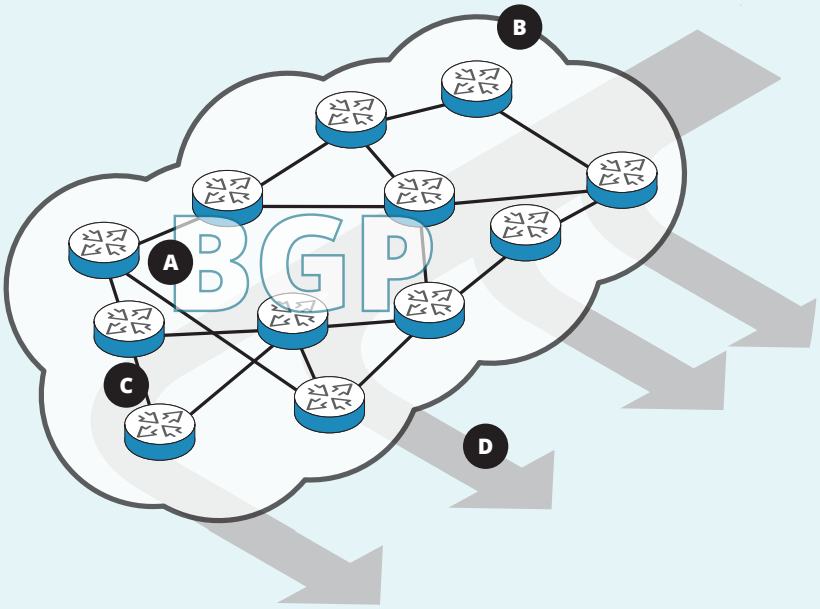
Learn more about GreyBox on Github. You can download it and use it in your emulations, change it to suit your needs, and send us your feedback.
github.com/cmu-sei/greybox

Installation Requirements

To use GreyBox, you must have a DHCP Server and the following software, all available on Github:

- TopGen
- CORE
- Quagga
- keepalived

Simply run the ./install.sh script to install GreyBox components on your filesystem. Review the ./contrib/greybox.spec for instructions about building a GreyBox RPM package.



GreyBox Highlights

A. Because the GreyBox Internet backbone emulation package provides TopGen connectivity, connections to web sites travel to the correct Tier 1 Internet providers via BGP.

B. TopGen solves the problem of providing Internet content for air-gapped networks by replicating the top 500 servers on the World Wide Web.

C. TopGen responds to requests from live users and non-player characters with simulated servers that appear to originate from different locations across the world.

D. Live users as well as non-player characters create traffic by sending requests to TopGen.

Explore Our Tools Online

SEI cyber training tools can be used to create cybersecurity training to help students learn in near-real-world situations without risking organizational assets.

See the latest information about these tools on our website at **sei.cmu.edu/go/cwd-tools**.

About the SEI

The Software Engineering Institute is a federally funded research and development center (FFRDC) that works with defense and government organizations, industry, and academia to advance the state of the art in software engineering and cybersecurity to benefit the public interest. Part of Carnegie Mellon University, the SEI is a national resource in pioneering emerging technologies, cybersecurity, software acquisition, and software lifecycle assurance.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu