FEDORA RED TEAM

A FEDORA PROJECT SPECIAL INTEREST GROUP

INTRODUCTION

The goal of the Fedora Red Team (FRT) is to become Red Hat's upstream cybersecurity community. This Special Interest Group (SIG) is the community focal point for offensive tooling, exploit curation, standards, and reference architectures.

> *"To be the catalyst in the enterprise Linux community that enables Computer Network Operations, the open source way."*
>
> FEDORA RED TEAM
> MISSION STATEMENT

The origins of the term "cyber" in relation to infosec can be traced back to the Greek verb, kubernao, meaning to steer or to govern. The Kubernetes project shares the same etymological root. Shortly after World War II, Norbert Wiener coined the term "cybernetics," meaning the "the scientific study of control and communication in the animal and the machine." Perhaps this served as inspiration to WIlliam Gibson, when in 1984 he wrote the classic cyberpunk novel, "Neuromancer," in which the global virtual reality realm was referred to as "cyberspace." Later in 1997, the Marsh Report, inspired by Gibson, used the term "cyber" to describe the digital domain.

More fomally defined, "cyber" could be described as Computer Network Operations (CNO). This umbrella term is comprised of Computer Network Defense (CND), Computer Network Exploitation (CNE), and Computer Network Attack (CNA).

The Fedora Red Team's mission is to be the catalyst in the enterprise Linux community that enables Computer Network Operations, the open source way. The SIG page is at https://fedoraproject.org/wiki/SIGs/Red_Team.

Join us on the first Friday of every month at 1400 UTC for our team meeting.

Freenode IRC **#fedora-security**

INITIAL PROJECTS

ENTERPRISE LINUX EXPLOIT MAPPER

The Enterprise Linux Exploit Mapper (ELEM) maps open CVEs on a local Linux system to known exploits in the wild. These exploits are curated, and scored in terms of effectiveness and ease of use. ELEM is useful to both defensive and offensive roles. From a defensive perspective, ELEM can be used to identify and patch super-critical vulnerabilites which have known exploit code available. Pen Testers can use ELEM to identify and practice working exploits, as well as to enumerate leverageable vulnerabilities on a system they are pen testing.

GitHub: https://github.com/fedoraredteam/elem | Demo: https://youtu.be/NX931nfyAmg

Fedora Security Blog
fedoraplanet.org/security

FEDORA CYBER TEST LAB

The Fedora Cyber Test Lab (FCTL) quantitatively analyzes binaries to assign a level-of-risk to each indicating how time consuming it would be to find a zero day in that binary. Scoring is based on cyclomatic complexity, branch frequency, hardening features such as function fortification or use of ASLR, and known-bad functions. This project is open source and repeatable, and should help developers adopt security best practices, and well as help security researchers focus on low-hanging fruit for new exploits.

GitHub: https://github.com/fedoraredteam/cyber-test-lab

Download Fedora Workstation, Server, or Atomic images
getfedora.org

fedoraproject.org

ROADMAP PROJECTS

There are other projects on the Fedora Red Team's roadmap.

FEDORA SECURITY DATA API

Fedora Security Data API provides CVE mappings and security data a la the Red Hat Security Data API. Refer to https://access.redhat.com/labsinfo/securitydataapi for details.

EXPLOIT CURATION

The Fedora Red Team will test vulnerability / exploit combinations and document the ones that can be leveraged by attackers. This curation will take place at https://github.com/fedoraredteam/elem-curation.

RED CONTAINER

Adoption of the Open Container Image Format is changing the packaging landscape. RPMs are still useful, but getting community adoption and participation in a containerization effort is easier than that of a packaging effort.

The Red Container project will work on containerizing the popular tooling in Kali Linux so that they can be run from any Linux distro, including Fedora, CentOS, and RHEL.

PEN TESTING EXECUTION STANDARD

The Fedora Red Team will participate in the Pen Testing Execution Standard (PTES). See http://www.pentest-standard.org/index.php/Main_Page for details.

REFERENCE ARCHITECTURES

The Fedora Red Team will document reference architectures for topics such as the Cyber Range and Next-Generation Malware Analysis designs, as well as publish Ansible playbooks for automated deployments.

CONTACT

There are several ways to contact the Fedora Red Team:

Email	jasoncallaway@fedoraproject.org k6n@fedoraproject.org nsabine@fedoraproject.org
IRC	#fedora-security on Freenode IRC
List	security@lists.fedoraproject.org
GitHub	https://github.com/fedoraredteam

ABOUT THE FEDORA PROJECT

The Fedora Project is a global partnership of free software community members. The Fedora Project is sponsored by Red Hat, which invests in our infrastructure and resources to encourage collaboration and incubate innovative new technologies. Some of these technologies may later be integrated into Red Hat products. They are developed in Fedora and produced under a free and open source license from inception, so other free software communities and projects are free to study, adopt, and modify them.

fedoraproject.org