

RESEARCH BRIEF

FERRET: AUTOMATED CHECKING FOR WINDOWS HOST VULNERABILITIES

The challenge

The research challenge is to develop a Microsoft Windows software package that checks for a wide variety of vulnerabilities on the host machine. This toolset should be open source, modular and easily extensible by developers. These requirements will allow the security community to collaborate on a software package that reflects a large set of vulnerability checks.

The potential

After reviewing these existing tools, Dr. Cukier concluded that there is a great need for a tool that covers a wide range of vulnerabilities, supports the addition of new modules, automates what system administrators are doing manually, and is free and open source. Such a tool would greatly benefit the security community.

The software tool

Ferret is a free, open-source host vulnerability finding toolset based on Java technology and the Visual Basic Scripting language. Ferret divulges all of its technology in an open source package available for inspection. This allows developers to be confident with the software running in their environment.

Ferret includes a core program, plug-in modules and output modules. The core program checks the operating system version, looks for dependencies, and runs the vulnerability checking and output modules. The modules detect vulnerabilities and produce an output in a specified format. For example, users can create a consolidated presentation of individual plug-in outputs in both text and HTML.

Currently, Ferret is equipped with over fifty plug-in modules covering a wide range of vulnerabilities. Each vulnerability checking plug-in performs only one action, such as checking for one vulnerability or listing the network file shares. The plug-ins are divided into vulnerability related subsections. These sections are: storage, security policies, domain set-

tings, local settings and passwords. In addition, as new vulnerabilities are discovered, Ferret's modularity allows new plug-ins to be quickly developed by the Ferret development team working with the security community. Ferret also supports the development of custom plug-ins by system administrators looking to automate tasks associated with setting up a new machine or troubleshooting problems on an older setup.

Current and future availability

Ferret is available online at ferret.sourceforge.net. Members of the security community are invited to both use the software and to develop new vulnerability checking modules. Dr. Cukier's research team will continue to develop new plug-in features and update existing ones.

Research team

Dr. Michel Cukier

Department of Mechanical Engineering
Center for Risk and Reliability
Institute for Systems Research affiliate
University of Maryland

Students

Matin Tamizi, Matt Weinstein, Daniel Ilkovich,
Doug Musser
University of Maryland

Support

This research was supported by NSF CAREER award 0237493.

Contact

Michel Cukier

Assistant Professor
Center for Risk and Reliability
Department of Mechanical Engineering
Institute for Systems Research affiliate
0151E Martin Hall
University of Maryland
College Park, MD 20742

Phone: 301.314.2804
Fax: 301.314.9601
Email: mcukier@umd.edu
www.enre.umd.edu/faculty/cukier.htm

Download

Ferret-Windows is freely available open-source software. Full documentation is available online. It can be downloaded at: ferret.sourceforge.net

Web links

Center for Risk and Reliability
www.enre.umd.edu/centers.htm

Reliability Engineering at the University of Maryland
www.enre.umd.edu