Ferret: A Host Vulnerability Checking Tool

Anil Sharma*, Jason R. Martin**, Nitin Anand*, Michel Cukier*, William H. Sanders**
* University of Maryland, ** University of Illinois http://ferret.crhc.uiuc.edu

Architecture Overview

Three main components of Ferret are:
- Management (Ferret core)
- Scanning agent (Vulnerability checking plug-ins)
- Collecting agent (Output plug-ins)

Ferret Design Goals

- Specific vulnerability checks
- Modular vulnerability checks
- Platform-independent
- Keyword-grouping of vulnerability plug-ins
- Modular output

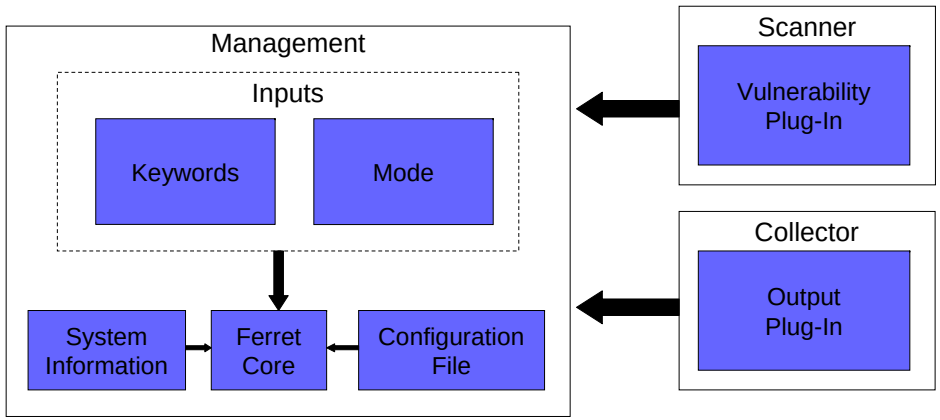
Ferret Core

- Designed and implemented in Perl
- Selects and runs individual vulnerability plug-ins based on keywords specified
- Feeds output of individual vulnerability plug-ins to selected output plug-in to produce scan report
- Generates reports in different formats

Ferret Core Procedure

- Interpret command line, read in config file
- Determine OS and version
- Determine what plug-ins are available
- Query plug-ins for meta-data
- Build hash table of plug-in keywords
- Determine which plug-ins to run based on keywords
- Run plug-ins
- Divide plug-ins into two categories: those that found vulnerabilities and those that did not
- Pipe output through the output plug-ins based on chosen mode and output format

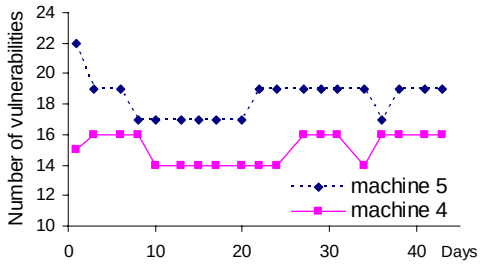
Ferret Architecture

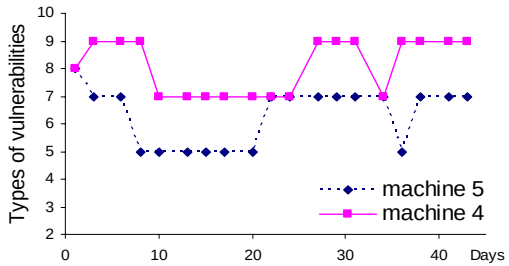


Experimental Results

- Ferret installed and run on six machines
- Data collected three times per week for 1.5 months
- Three server-class machines and three workstations

Machine	Operating System	OS Version	Machine Function	Types of Vulnerabilities	Number of Vulnerabilities	Execution Time (sec)
1	Linux	RH7.2 + Updates	Workstation	22	102	146
2	Sun Solaris	5.8 (Solaris 8)	Workstation	2	4	29
3	Sun Solaris	5.8 (Solaris 8)	Server (NIS, NFS, RPC)	12	14	234
4	Sun Solaris	5.8 (Solaris 8)	Server (NIS, NFS, RPC)	8	19	180
5	Sun Solaris	5.7 (Solaris 7)	Workstation	6	15	25
6	HP-UX	B.10.20	Server (NIS, NFS, DNS, DHCP, Mail)	35	303	111





Vulnerability Checking Plug-ins

- Designed to scan for one specific vulnerability
- Interact with the Ferret core using command line options
- Currently about 80 plug-ins implemented
- Can be divided into nine groups
  - Critical system files/directories are owned by root
  - Critical system files/directories are world writable
  - Paths and filenames in root start-up files world writable
  - Umask settings in start-up files
  - Configuration file permissions in user home directories
  - SUID file permission checks
  - Password file configuration issues
  - Exported filesystem and mounted filesystem configurations
  - .rhost file settings

Output Plug-ins

Output plug-in can be run for two different modes

First Mode
- Vulnerability information (name of plug-in, short description of the plug-in, result of the scan)

Second Mode
- Vulnerability information (name of plug-in, result of the scan)
- Vulnerability exploitation information (builds privilege graph)