Central Firewall Management as a Method of Improving Security

Branson Matheson
branson@sandsite.org

Introduction

- Branson Matheson
- Computer Security for 20 years
- Involved with SANS, Shmoo, many OSS projects
- Worked for NASA, TSA, DoE, DoT, most of the beltway bandits

Topics

- Scope
- Security as a function of C
- Central Control
- Difficulties
- Solutions
- fwbuilder
- Discussion
- Demo
- Q&A

Scope

- Host vs. Network Security
- Risk Management
- Bastions
- Segregation
- Detection

Security as a Function of C

- Confidentiality of Data
  - Data Type Reasons
  - Legal Reasons
- Confidentiality of Exposed Information
  - Reputation
  - Vulnerability

Central Control

- IPS vs IDS
- Management Tools
- Scripts
- Revision Control

Difficulties

- Different types of Network Devices
  - Routers, Firewalls, Switches
- Different configuration formats
  - IOS, Unix, ipfw, pf, etc..
- Different configuration paradigm
- Keeping it all straight

Solutions

- Consolidation one vendor
  - cisco, juniper, linux (switches?) etc..
  - What about my end points?
- Expensive integrated solutions
  - cisco, norton, etc..
  - What about my bottom line?

Solution

- One tool for managing all edge and bastion systems
- One tool that crosses netgear platforms (cisco, OSS, etc.)

- Fwbuilder

fwbuilder

- About
- History
- Current State
  - –

Fwbuilder
OS Distributions and Versions

Linux	Debian, Ubuntu, RedHat, Fedora, Mandrake, SuSe
Solaris	8
FreeBSD	in ports
OpenBSD	in ports
Mac OS X	Leopard and Snow Leopard
Windows	2000, XP, Vista

Fwbuilder
Supported Firewalls

Firewall	OS
iptables	Linux (kernel 2.4.x and 2.6.x), including OpenWRT, DD-WRT,
Sveasoft	firmware for embedded systems
ipfilter	FreeBSD, OpenBSD, Solaris
ipfw	FreeBSD, MacOS X
pf	OpenBSD 3.x, 4.x
Cisco PIX	Cisco ASA appliance (PIX) v6.x, 7.x, FWSM module
Cisco IOS	IOS v12.x

Discussion

- Objects
- Rule Creation
- NAT Creation
- Ruleset Validation
- Fallback Rules

Discussion

- Posting Rules to devices
  - SSH (yay!)
- Version Control

Discussion

- Quick and Dirty
- Druids vs. Trees

Demo

Q&A

As Bs and Cs