Intro to ADIOS

Cecil Hornbaker
September 21, 2005

Forensig LUG
http://forensiclug.com

Topics

- Why ADIOS
- Overview of ADIOS distribution and Live CD
- Forensic LUG Lab: fluglab
- Discussion about fluglab
- References

Why ADIOS?

- I wanted to create a virtual lab with SELinux and UML to learn experiment to learn these and experiment with forensic tools
- I'm too lazy to do it myself so I search for a distribution – ADIOS has it all
    - Live CD
    - SELinux
    - UML
    - Forensic tools

ADIOS Topics

- ADIOS distribution and Live CD basic contents
- SELinux in ADIOS
- UML in ADIOS
- Forensic tools in ADIOS

ADIOS Distribution and Live CD

- Created by Neville Richter, Queensland University of Technology
- ADIOS distribution is built for teaching labs
- ADIOS distribution based on Fedora Core 3
- ADIOS is a Live CD
- ADIOS 4.13 includes
  - kernel 2.6.12 with SELinux and UML support
  - X, KDE (or GNOME, XFCE, ICE)
  - forensic tools

ADIOS SELinux

- ADIOS 4.13 SELinux
  - FC3 SELinux support compiled in kernel
  - SELinux setools package installed
  - SELinux targeted policies installed
- SELinux UML kernel
  - ADIOS 4.13 has SELinux kernel option for UML kernel
  - Setools and targeted policies

ADIOS SELinux (cont)

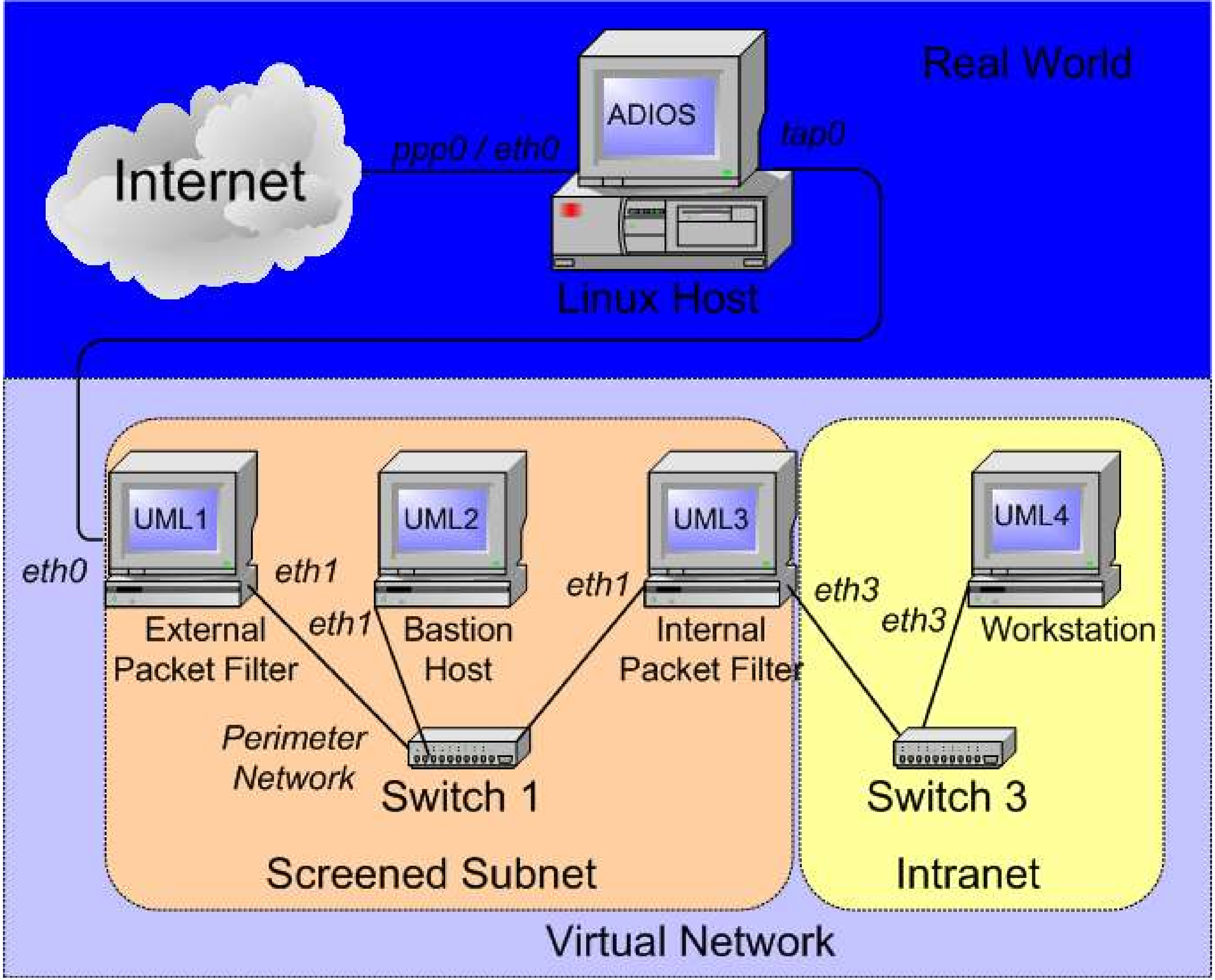
- SELinux targeted policies
  - Controls what access is available to certain system services
  - Minimizes harm if service security flaw is exploited
  - Does **not** provide restrictions on what root and users can do beyond normal Linux permissions

ADIOS UML

- ADIOS has User Mode Linux kernel support
- ADIOS supplies UML scripts and config files
  - /opt/uml/bin/uml is main command to start/stop uml instances with options
- Typical UML config/options
  - 64 MB RAM
  - 500 MB Disk
  - filesystem options, Copy-on-Write (COW)
  - LIDS/SELinux options
  - console: shell, xterm, tty

ADIOS UML (cont)

- ADIOS UML virtual networking
  - private virtual network
  - 1 virtual hub, 4 virtual switches (number is configurable)
  - NAT routing through host for LAN/Internet access



* Diagram from Neville Richter presentation

ADIOS Forensic Tools

- ADIOS Forensic Tools Packages
  - autopsy
  - sleuthkit
  - nagios (network monitoring program)
  - nessus (security scanner)
  - snort
  - acid (analysis console for incident database)
  - mrtg

Forensic LUG Lab Topics

- Forensic LUG Lab (fluglab) – Live online system for Forensic LUG users
- System hardware and ADIOS configuration
- ssh access via fluglab.no-ip.org
- Rules for usage
- Help with administration

Forensic LUG Lab

- Forensic LUG Lab (fluglab)
- Live online system
  - PC: 1.x GHz CPU, 1 GB RAM, 80 GB Disk
  - ADIOS 4.13-pre1 ISO on hard disk
  - /var on hard disk partition
  - headless: boots to runlevel 3 (text mode)
  - should easily support 8 96 MB UML instances with light load (8 x 96 MB -> 768 MB, leaves 256 MB for host)

Fluglab Access

- Installed in DMZ with Internet access
- Access via ssh:
  - ssh -p 10022 adios@fluglab.no-ip.org
  - must use port 10022, ssh to default port is a different system
  - root login via ssh disabled
- DEMO
  - ssh -p 10022 adios@fluglab.no-ip.org
  - ./start-uml

Fluglab Rules

- Goal is open access
  - Problem: control abuse if system is cracked
    - SELinux targeted policy doesn't provide protection
    - Need to work to get strict policy working
  - Compromise: user accounts for flug members
    - Use intrusion detection tools to monitor
    - Don't store sensitive data or data that can't be lost
    - Inform admins if security holes are found

Fluglab Admin Help

- Need admin help
  - Setup intrusion detection, monitoring
    - Automatic shutdown if system is cracked
  - Administer forensiclug users
  - Administer UML instances for fluglab activities
  - ***Setup strict selinux policy***

Fluglab Discussion

- What to do with fluglab?
  - Use UML instances with virtual network to do hands on play with forensic tools
    - UML1 – target system
    - UML2 – run intrusion detection
    - UML3 – attack target system
    - etc
  - Other ideas

References

- ADIOS
  - http://dc.qut.edu.au/adios/
  - http://dc.qut.edu.au/adios/adk/index.html
- SELinux
  - http://www.coker.com.au/selinux/
  - http://www.nsa.gov/selinux/index.html
- UML
  - http://user-mode-linux.sourceforge.net/index.html
  - http://usermodelinux.org/