Linux Operating System Security

Kenneth Ingham and Anil Somayaji

September 29, 2009

1 Course overview

This class is for students who want to learn how to configure systems to be secure, test the security of systems, and/or and manage the system more securely.

2 Course objectives

- Know how to work with a network mapping tool and how to control what it discovers.
- Know how to work with penetration testing systems and how to reduce their threat.
- Understand network security issues and how to control network access.
- Learn about some of the intrusion detection systems available.
- Understand how the use of cryptography can improve system security, including topics such as VPNs, SSL/TLS, and OpenSSH.
- Understand local operating system security issues, such as logging, file permissions, password security, and the setuid bit.

3 Student background

If you are attending this class, then we assume that

- You should have a basic familiarity with Linux system administration. Specifically:
  - When a lab says, "install the RPM foo.rpm" or "install the package in foo.tar.gz", you should understand what this means and how to do it.
  - You should understand Unix file permissions, how they work, and how you change them.
  - You should understand how to create users and the parts of a user account.

  - You should understand the process the system goes through when it boots.

- Knowledge of shell programming will help you understand the system startup scripts, etc.

- If you know regular expressions, you will be able to make better use of the various tools that use them for searching.

- (For optional kernel chapter) You should understand how to build a new kernel (although the class notes will give some guidance on this topic).

4 Logistics

The class lasts three days. Fedora Core 4 The class uses the following software:

- Apache web server
- Bastille Linux RPM
- CentOS 5.x or Red Hat Enterprise 5.x
- Firefox (on Linux distribution but needed for Windows)
- GnuPG
- IP Tables and associated kernel modules and any GUI config tools.
- Kernel sources from kernel.org or distribution
- LIDS distribution to match the kernel
- OpenSSL command-line utilities
- PAM
- Perl-Tk and Perl-Curses RPMs
- TCP wrappers
- *aide* (on OS distribution)
- *bzip2*
- *chattr*
- *chmod*
- *find*
- *fuser*
- *iptraf* (if covered in this class)
- *logger*
- *logrotate*
- *lsattr*
- *lsof*
- *mke2fs*
- *mount*
- *named* manual page; a web browser with Internet access
- *nessus* client and server either installed or distribution files available
- *netstat*

- *nmap*
- *nmap* (on distribution media)
- *portsentry* (installed or distribution files)
- *snort* installed or distribution files
- *socklist*
- *sshd*
- *ssh*
- *stunnel* version ≥ 4.0
- *sudo*
- *syslogd*
- *telnet* (client)
- *umount*
- *xinetd*
- *xinetd* or *inetd*
- ***pam_wheel.so***
- a DHCP and DNS server for the class
- a ***/test*** filesystem (size not critical) for mounting nosuid and/or nodev.
- an NIS server on the instructor machine with an account the students will log into (if this class covers NIS)
- ipsec-tools
- static IP addresses (these do not need to be routable)

No class network information specified.

The class needs a web server for the class web site. The instructor's laptop may be this web server; otherwise the machine provided in the classroom for the instructor is a good choice. This machine obviously will need web server software installed.

5 Class outline

1. Introduction (Lecture: 15; Lab: 0)
   (a) Class Introductions
   (b) Class Logistics
      i. Class schedule
      ii. Breaks
      iii. Question policy
      iv. Break room and restroom locations
      v. Assumptions about your background
   (c) Typographic conventions
   (d) What the class covers
2. General Security Issues (Lecture: 25; Lab: 30)
   (a) General OS security

        i. Physical security is paramount
        ii. Security is a process, not a product
        iii. Fewest services/minimal functionality
        iv. Least privilege
        v. Compartmentalization
        vi. Defense in depth
    (b) Patches and keeping current
    (c) Security myths
        i. "We have a firewall, the attackers cannot get to this machine"
        ii. "I use anti-virus software; my machine does not have any malware"
    (d) Class software
    (e) Summary
    (f) Lab
3. Logging (Lecture: 30; Lab: 35)
    (a) Overview
    (b) *syslogd*
        i. ***syslog.conf***
        ii. Facilities
        iii. Severity Levels
        iv. Actions
    (c) Log file rotation
        i. *logrotate* directives
    (d) Utilities to assist with log files
    (e) Summary
    (f) Lab
4. Authentication (Lecture: 45; Lab: 45)
    (a) Password cracking
    (b) PAM
        i. Example
    (c) Root access
    (d) *sudo*
        i. *sudo* configuration
    (e) nsswitch.conf
    (f) Kerberos
        i. Quick Overview
        ii. Session Protocol
        iii. Setting up a Kerberos server
        iv. Setting up a Kerberos client
    (g) LDAP

        i. Setting up an LDAP server
        ii. Using LDAP as a client
    (h) Summary
    (i) Lab
5. Local security issues (Lecture: 20; Lab: 60)
    (a) Disk partitioning
    (b) Setuid files
    (c) The sticky bit on a directory
    (d) Local security scanners
        i. *rpm* verification
            A. Limits of *rpm* verification
    (e) Summary
    (f) Lab
6. nmap and network mapping (Lecture: 20; Lab: 40)
    (a) *nmap* overview
    (b) Using *nmap*
    (c) *netstat*
    (d) *lsof* and *fuser*
    (e) Summary
    (f) Lab
7. Penetration testing (Lecture: 15; Lab: 60)
    (a) Testing for security
    (b) *nessus*
        i. Installing and running *nessus*
    (c) Other non-commercial penetration testing tools
    (d) Commercial penetration testing tools
    (e) Summary
    (f) Lab
8. Network access control (Lecture: 50; Lab: 60)
    (a) Introduction
    (b) TCP wrappers
    (c) xinetd
    (d) IP Tables
        i. OS details
        ii. Basic IP tables commands
        iii. Rules
        iv. *iptables* examples
    (e) GUI configuration tools
    (f) Troubleshooting

(g) Summary
(h) Lab

9. Intrusion Detection Overview (Lecture: 25; Lab: 35)
   (a) Introduction
   (b) Types of Intrusion Detection Systems
      i. Input data stream
      ii. Data analysis method
      iii. Response strategy
      iv. Honeypots and darknets
   (c) Evaluating IDS systems
   (d) Comparing IDS strategies
   (e) IDS Overview Lab
10. Host-based Intrusion Detection Systems (Lecture: 20; Lab: 65)
   (a) Introduction
   (b) *aide*
      i. Using *aide*
   (c) *tripwire*
      i. Configuring Tripwire
   (d) *portsentry*
      i. Installing and configuring *portsentry*
   (e) Other open source host-based IDSs
   (f) Commercial products
   (g) Summary
   (h) Lab
11. Network Intrusion Detection Systems (Lecture: 15; Lab: 45)
   (a) Introduction
   (b) *snort*
      i. Installing *snort*
      ii. Configuring *snort*
      iii. Running *snort*
   (c) Other NIDSs
   (d) Lab
12. SELinux (Lecture: 35; Lab: 30)
   (a) Overview of SELinux
   (b) Discretionary versus mandatory access control
   (c) SELinux vocabulary
   (d) Security contexts
      i. Overview

        ii. Example
        iii. Processes
        iv. Files and filesystems
    (e) Security policies
    (f) Enabling SELinux
    (g) Working with file contexts
    (h) Handling SELinux denials
    (i) SELinux notes
    (j) Summary
    (k) Lab
13. Cryptography Overview (Lecture: 70; Lab: 55)
    (a) Introduction
        i. Cryptographic Applications
        ii. Open design
    (b) Cryptographic Primitives
        i. Cryptographic hash functions
        ii. Symmetric key encryption
        iii. Public key encryption
    (c) Digital signatures
    (d) Public Key Management
        i. The Problem
        ii. Certificates
        iii. Trust Models
        iv. Example: PGP/GnuPG
        v. Example: SSL/TLS
        vi. Overview
            A. The server
            B. The client
    (e) Random numbers
    (f) Parameter sizes
    (g) Insecure Cryptography
        i. Key management errors
    (h) Do not innovate in cryptography
    (i) Summary
    (j) Lab
14. Cryptographic Tools (Lecture: 40; Lab: 45)
    (a) Introduction
    (b) GnuPG digital signatures
        i. Example: Obtaining a key from a key server
        ii. Verifying PGP signatures

iii. Verifying package signatures with *rpm*

(c) *ssh*

i. Public key authentication
ii. Tunneling
iii. ssh client issues
iv. ssh server issues

(d) Lab

15. SSL and TLS (Lecture: 30; Lab: 60)

(a) Overview
(b) The server
(c) The client
(d) OpenSSL
(e) SSL/TLS configuration for servers

i. Apache
ii. SMTP AUTH and STARTTLS
iii. *stunnel* ≥ 4.0
iv. *stunnel* configuration file

(f) SSL/TLS issues in web browsers
(g) Important Points
(h) Lab

16. IPsec (Lecture: 30; Lab: 60)

(a) Introduction
(b) How IPsec works
(c) IPsec implementations for Linux
(d) ipsec-tools
(e) IPsec issues
(f) VPN Security
(g) Summary
(h) Lab

Appendices

A. Review of networking concepts (Lecture: 15; Lab: 0)

(a) ISO model of networking

i. Network layer addressing

(b) UDP
(c) TCP

i. TCP connection setup

(d) ICMP

B. Loop filesystem (Lecture: 0; Lab: 0)

(a) Loop device

C. Security packages and distributions (Lecture: 20; Lab: 20-140)

(a) Bastille Linux
(b) LIDS
(c) OpenWall
(d) Trustix Secure Linux
(e) Debian
(f) OpenBSD
(g) Lab

D. Kernel configuration options (optional) (Lecture: 20; Lab: 105)

(a) Kernel modules
(b) *lcap*
(c) Lab

E. Network Configuration (Lecture: 30; Lab: 45)

(a) Network configuration
    i. DHCP client configuration
    ii. Static network configuration
(b) DNS lookups
    i. ***/etc/resolv.conf***
    ii. *host*
(c) Virtual network interfaces
(d) *mii-tool* and *ethtool*
    i. Examples
(e) *system-config-network*
(f) Troubleshooting
(g) Summary
(h) Lab

F. Network services (Lecture: 30; Lab: 45)

(a) *xinetd*
(b) *ssh*
    i. Public key authentication
    ii. Tunneling
(c) NFS
    i. Client
    ii. Server
(d) Automounter
(e) Troubleshooting
(f) Summary
(g) Lab