

Introduction To Security

Lecture 3 – Securing a Linux Install

Martin Brain

University of Bath

May 19, 2006

The Course

- Week 1 Introduction to Security –
Concepts, Tools, Techniques
- Week 2 Case Study – Secure Shell
- Week 3 Case Study – Securing a Linux Install

Introduction

Network Security

Local Security

Application Security

Planning for the Worst

Things Were Not Going to Talk About

- ▶ Policy / Threat Model
- ▶ Physical Security
- ▶ Theory
- ▶ Legality and Ethics

Introduction

Network Security

Local Security

Application Security

Planning for the Worst

Disable Services

- ▶ Disable *all* unnecessary services.
- ▶ `netstat -ap`
- ▶ NMAP

Firewall

- ▶ Linux has had an inbuilt firewall since at least 1998
- ▶ Has a series of *tables* each of which has a *chain* of *rules*
- ▶ Needed?
- ▶ Some applications have their own controls

TCPWRAPPERS

Introduction

Network Security

Local Security

Application Security

Planning for the Worst

Updates

- ▶ Vital
- ▶ Each distro has their own mechanism ...
... use it!
- ▶ Join the relevant announcements list
- ▶ Vital

Users and Passwords

- ▶ 1 account per person, 1 person per account
- ▶ Set passwords to expire
- ▶ Passwords must not be predictable ...
- ▶ ... there are systems to enforce this and alternatives

Files and Permissions

- ▶ Permissions (UMASK)
- ▶ suid, sgid
- ▶ Exact permissions are complicated but mostly done automatically
- ▶ TRIPWIRE
- ▶ Many other tricks;
mount /tmp noexec, /home nosuid, sections read only, ...

Introduction

Network Security

Local Security

Application Security

Planning for the Worst

Sandboxes

- ▶ CHROOT
- ▶ Dropping priviledges
- ▶ SYSTRACE
- ▶ Virtualisation

Source(s)

- ▶ Only install software from 'trusted' sources.
(Digital signatures)
- ▶ Consider the security history of the application
- ▶ Only open source software?
- ▶ Code auditing - STRACE, LTRACE, SYSTRACE, BOOMERANG,
...

Specific Applications

- ▶ HTTP – APACHE
(but what about PHP ...)
- ▶ SMTP – EXIM
- ▶ SQL – MYSQL
- ▶ RPC – NFS, NIS
- ▶ SSH
- ▶ FTP, telnet, rlogin, inetd

Anti Virus

- ▶ “Next year will be the year of the Linux virus”
- ▶ Carrier?
- ▶ Clam AV / commercial

Introduction

Network Security

Local Security

Application Security

Planning for the Worst

Planning for the Worst

- ▶ Unplug → Authorities → Recover
- ▶ Verify scope and scale of damage
(static binaries and kernel on removable media)
- ▶ Identify attack vector
- ▶ Rebuild from scratch
- ▶ ... which is easy as you take regular backups

Striking Back...

- ▶ Honeypots
- ▶ Honeynets
- ▶ Tarpits
- ▶ (Ethics)

Questions?

Questions?

Made using only Free Software

Thank you for inviting me and thank you for attending