Securing Linux Systems with AppArmor

Crispin Cowan, PhD
Director of Software Engineering
Security Architect, SUSE Linux

Novell®

AppArmor:
~~Easy-to-use Security for Ubuntu Linux~~

Crispin Cowan, PhD
Security Architect, SUSE

What Is This 'AppArmor' Thing and Why Should I Care?

Novell®

Agenda

- Overview
- A Closer Look at AppArmor
- Deployment Scenarios
- Demonstration of AppArmor
- Competitive Positioning
- AppArmor Futures

Software Security Problem

Problem: Imperfect software :-)

- Reliable software does what it is supposed to do
- *Secure* software does what it is supposed to do, *and nothing else*

Solution: only use perfect software

... slight supply problem :-)

AppArmor Solution

Enforce that applications only get to do what they are supposed to do

What means “do”?

- At ultimate detail, this is the code itself
- But we clearly can't get that right :-)
- Need something simpler, more abstract

Resources:

- Restrict the application to only access the OS resources it should need

What Would You Do With That?

Make a server *network secure*:

- Confine all programs with open network ports
- If all open ports lead to confined processes, then you have completely defined policy for what a network user or attacker can do
- Yet *far* from having created policy for thw whole system

Is that really secure?

Hard to say

Security is semi-decidable

- You can only tell when something is *insecure*
- Hence all the Defcon talks on breaking something, and few on securing something

So lets put it to a practical test

- Put it in competition at Defcon and let people beat on it

Defcon CtF 2002-5 *a la* Ghettohackers

Some real-world red teaming

Play an Immunix server in the Defcon Capture the Flag (CtF) games

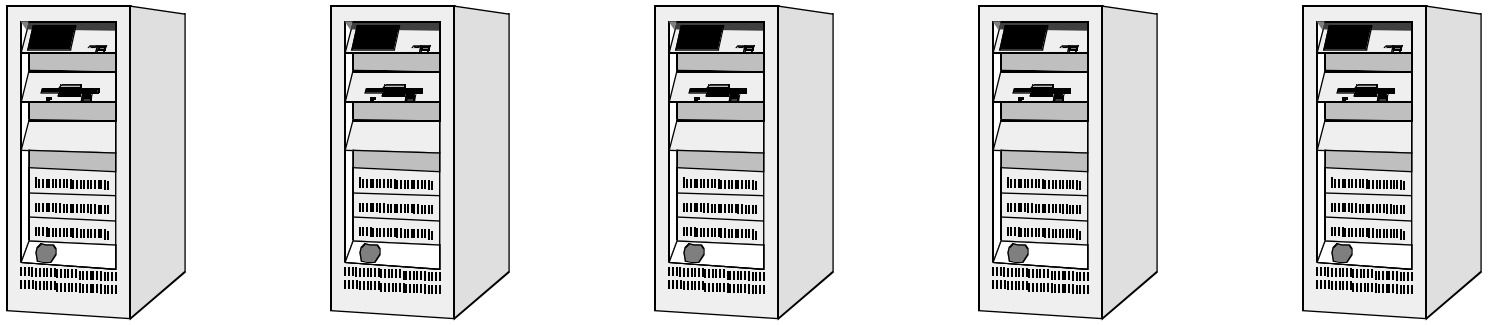
Almost no holds barred:

- No flooding
- No physical attacks

New gaming rig designed by the Ghettohackers

ghettohackers.net

Basic Defcon CtF Rules

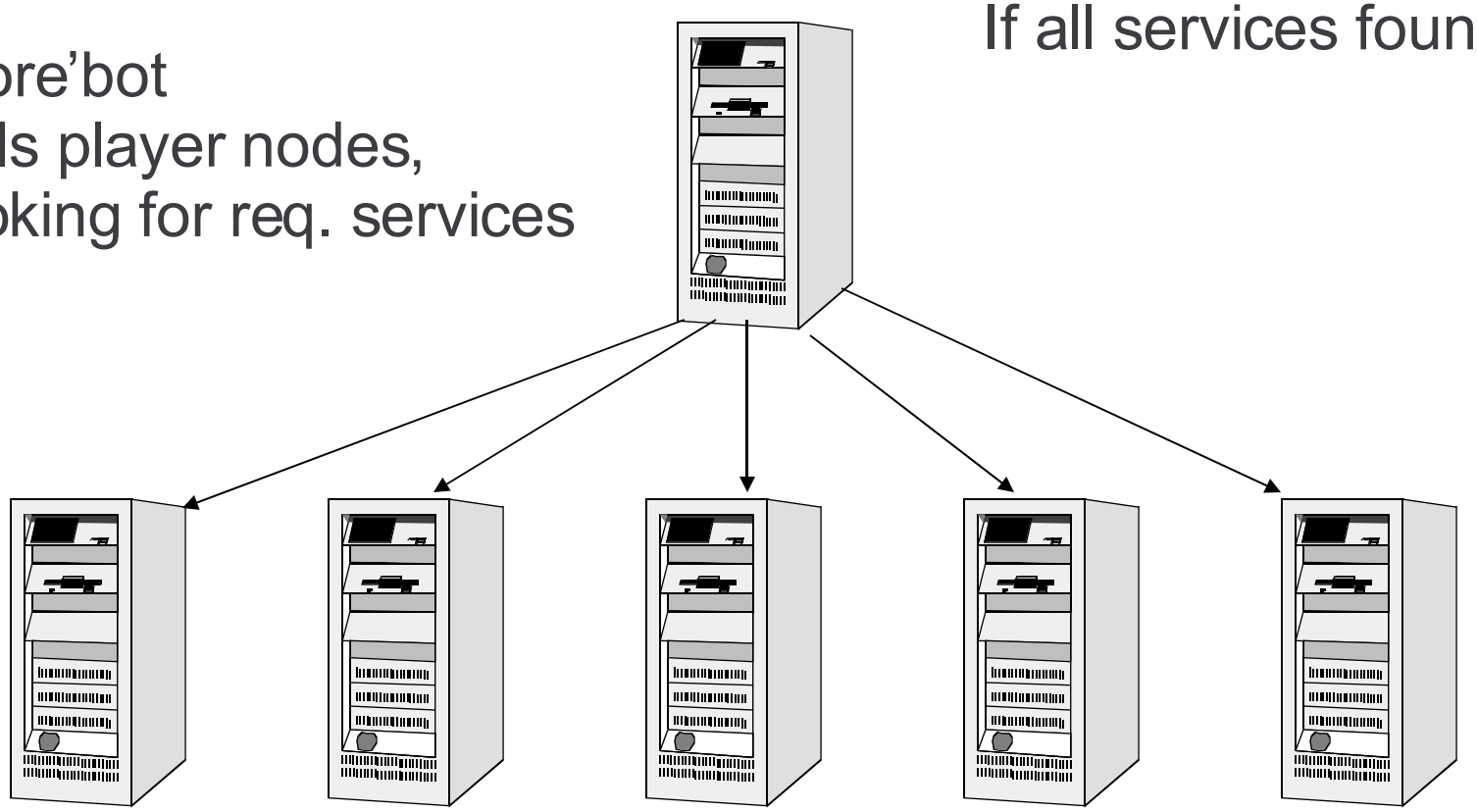


Player Nodes

Basic Defcon CtF Rules

Score'bot
Polls player nodes,
Looking for req. services

If all services found ...

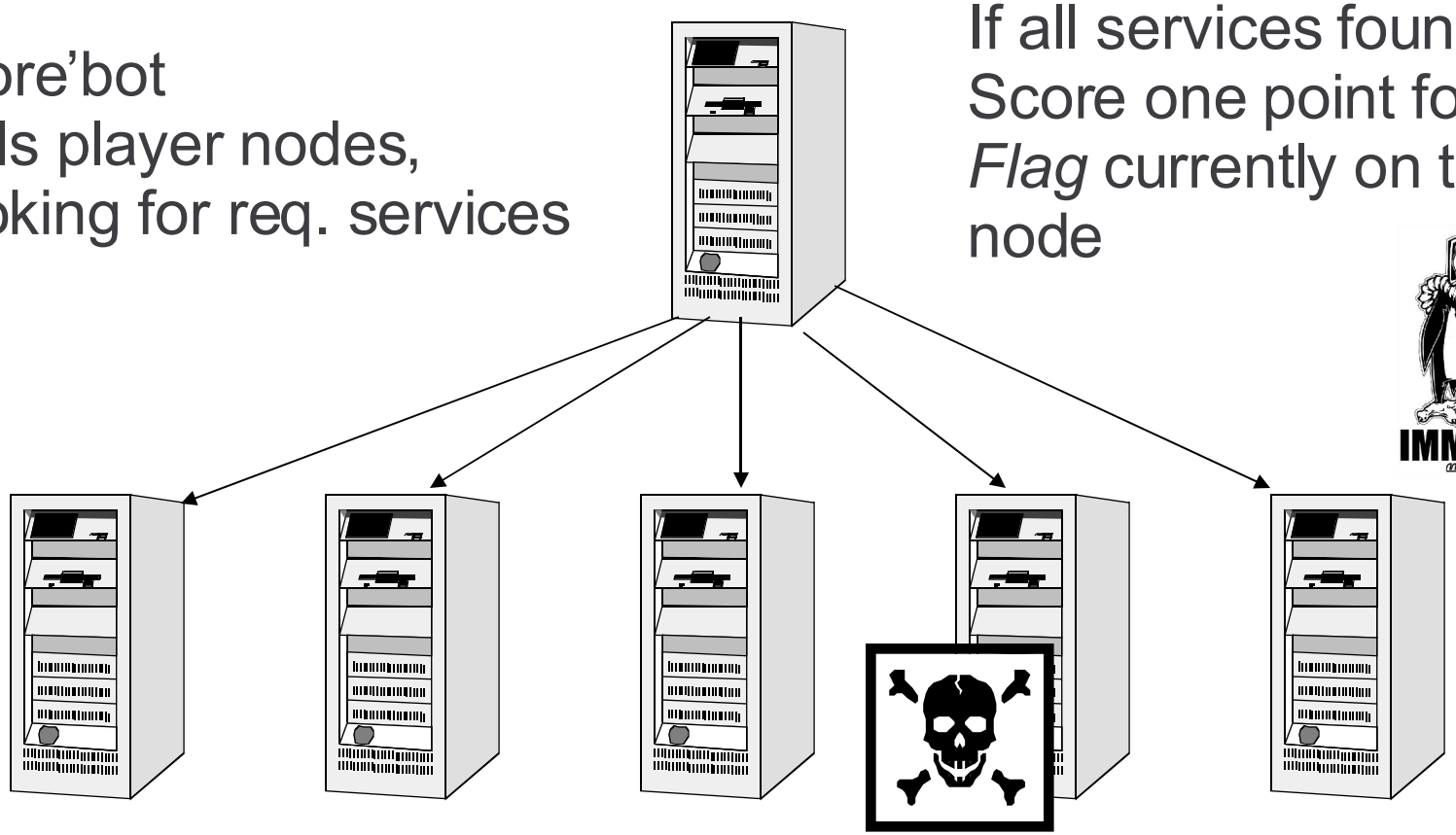


Player Nodes

Basic Defcon CtF Rules

Score'bot
Polls player nodes,
Looking for req. services

If all services found,
Score one point for the
Flag currently on that
node

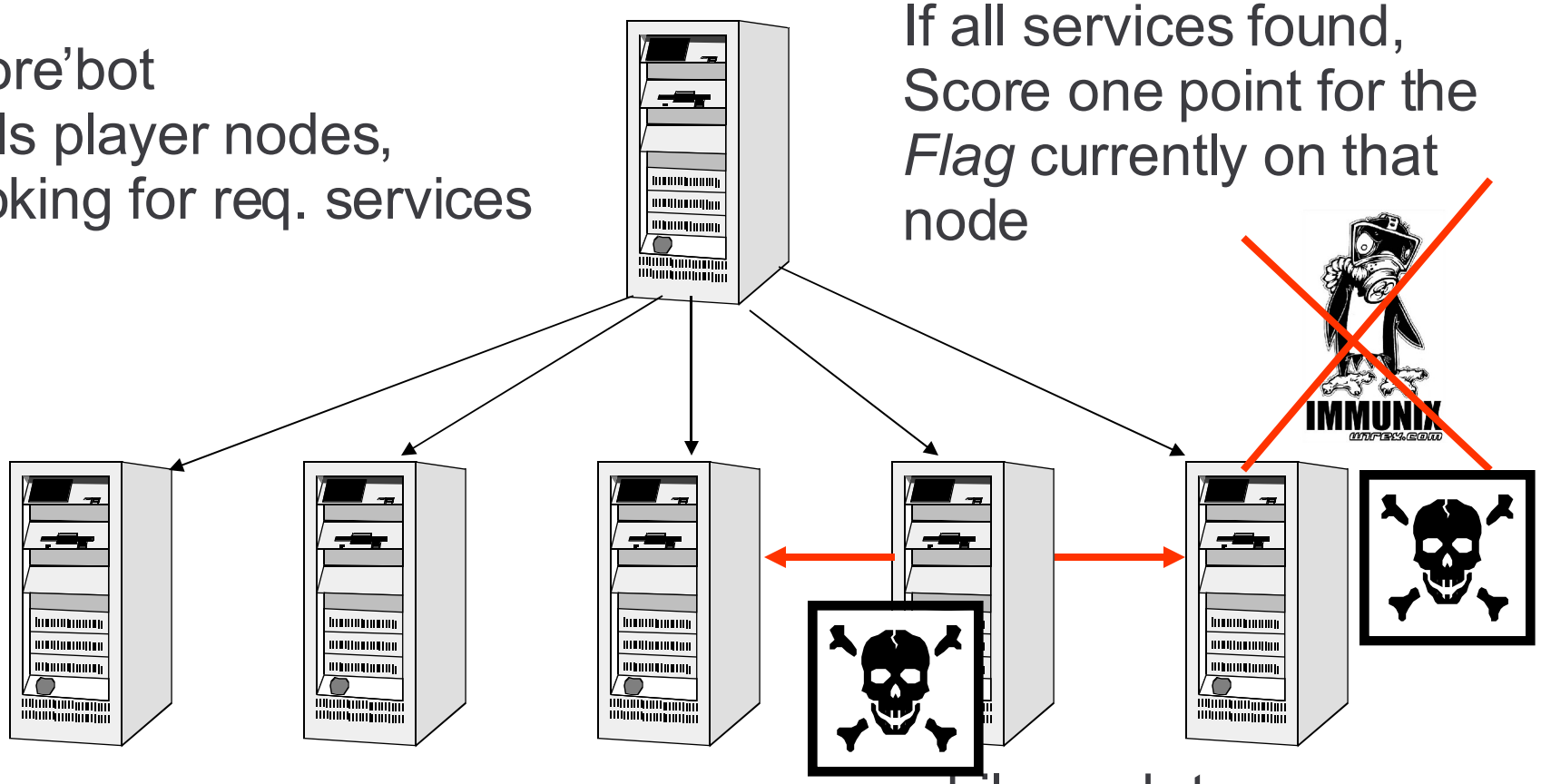


Player Nodes

Basic Defcon CtF Rules

Score'bot
Polls player nodes,
Looking for req. services

If all services found,
Score one point for the
Flag currently on that
node

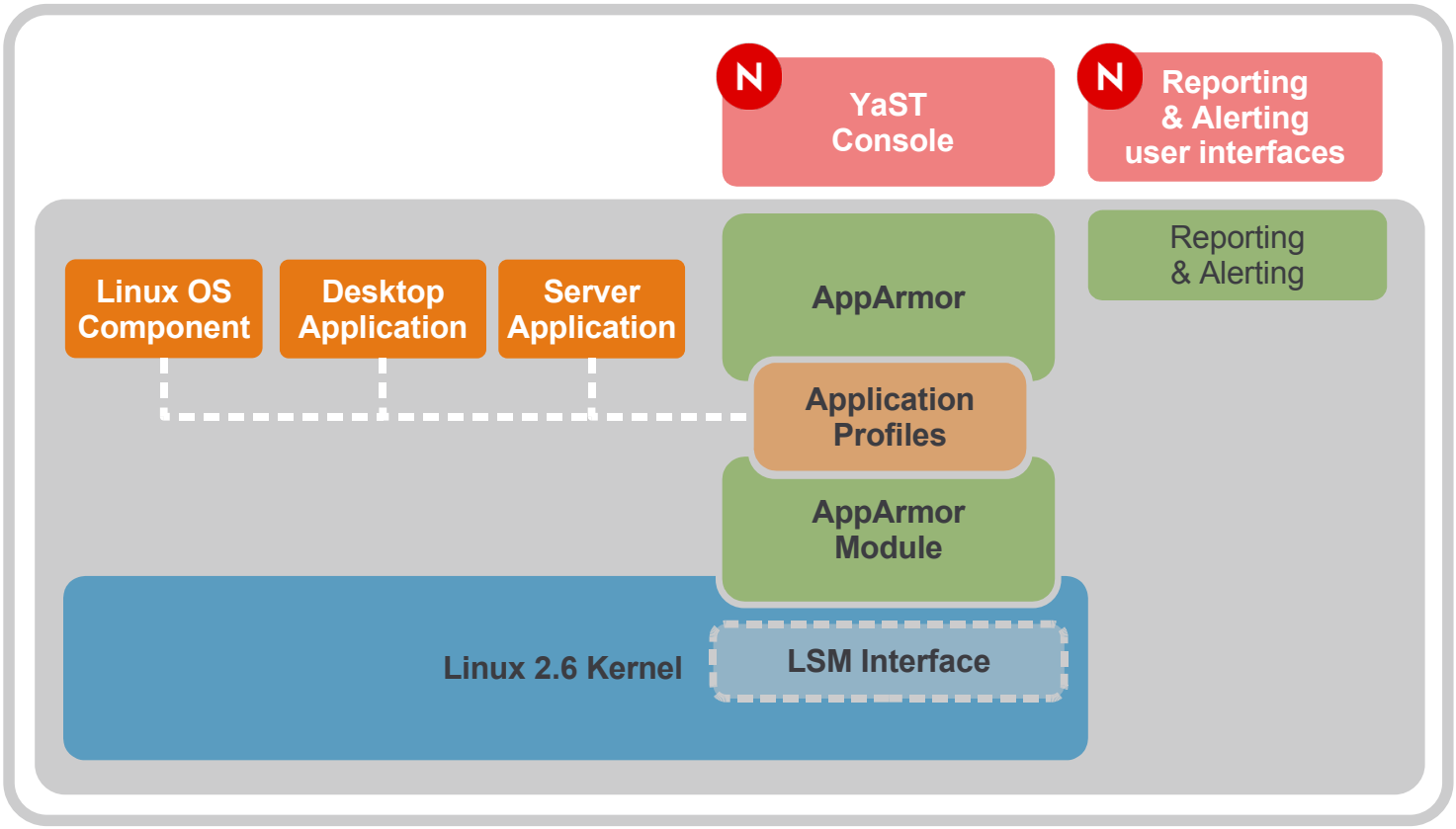


Player Nodes

… while each team
tries to replace others' flags

AppArmor
A Closer Look

AppArmor Architecture



Critical Issue #1: Complete Mediation

Must not be possible to bypass HIPS system

- Must be in the kernel

AppArmor uses LSM interface in 2.6 kernel

- LSM (Linux Security Module) provides in-kernel mediation without having to maintain a patched kernel
- Provides an open standard API for access control module
- Precise information on application behavior, accuracy, performance
- Provides highest quality non-bypassable mediation

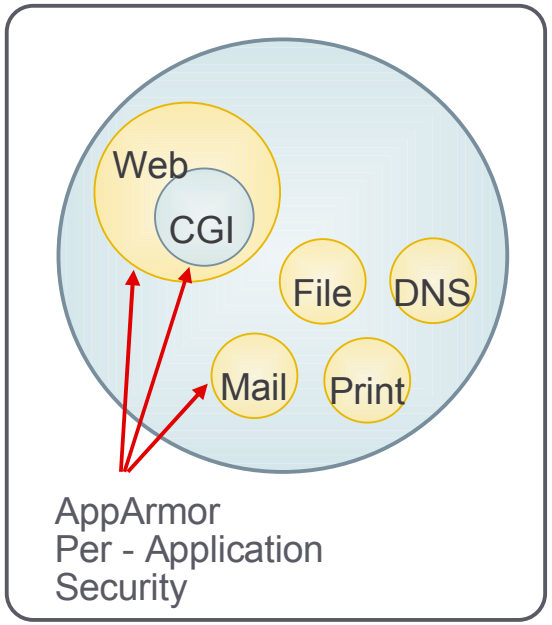
Critical Issue #2: Security Model

Misuse prevention vs. anomaly prevention

- Misuse prevention easier to manage
- Anomaly prevention much more secure, traditionally **hard** to use

AppArmor is easy anomaly prevention for application security

- Focus on *application* security
- Name-based access control for ease of understanding policy
- Hybrid white list/black list
  - White list *within* an application profile
  - Black list system-wide



AppArmor Security Profile

Whenever a protected program runs regardless of UID, AppArmor controls:

- The POSIX capabilities it can have (even if it is running as root)
- The directories/files it can read/write/execute

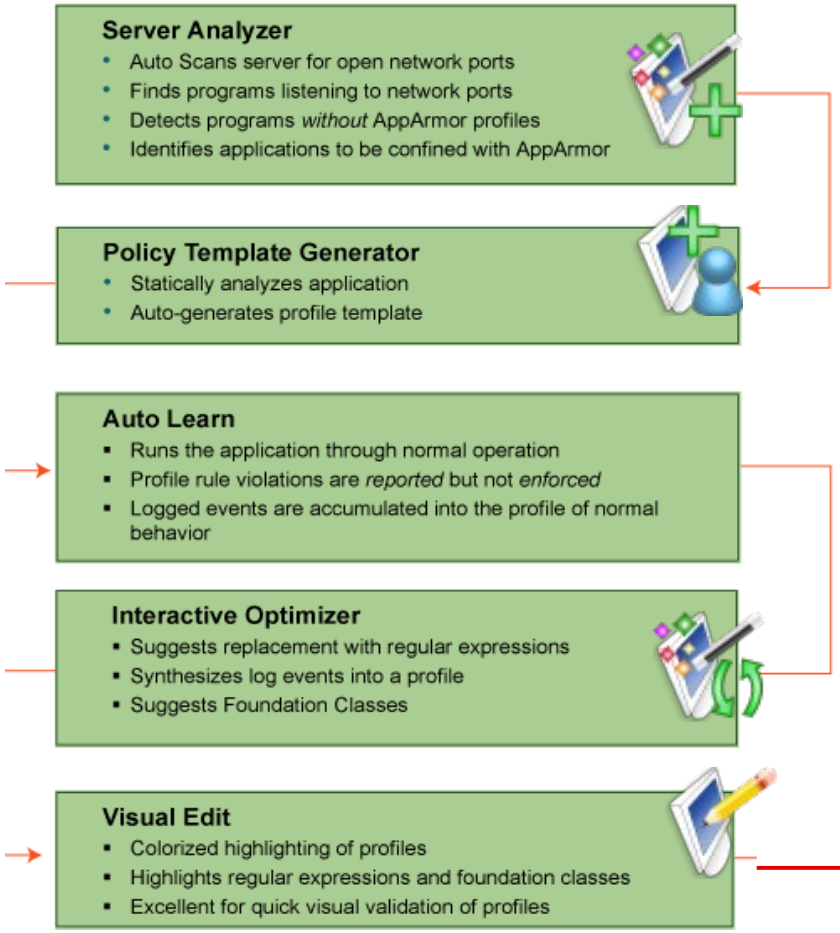
Example security profile for **ntpd**

```
/usr/sbin/ntpd {
  #include <abstractions/base>
  #include <abstractions/nameservice>

  capability ipc_lock,
  capability net_bind_service,
  capability sys_time,
  capability sys_chroot,
  capability setuid,

  /etc/ntp.conf                          r,
  /etc/ntp/drift*                        rwl,
  /etc/ntp/keys                          r,
  /etc/ntp/step-tickers                  r,
  /tmp/ntp*                              rwl,
  /usr/sbin/ntpd                         rix,
  /var/log/ntp                           w,
  /var/log/ntp.log                       w,
  /var/run/ntpd.pid                      w,
  /var/lib/ntp/drift                     rwl,
  /var/lib/ntp/drift.TEMP                rwl,
  /var/lib/ntp/var/run/ntp/ntpd.pid      w,
  /var/lib/ntp/drift/ntp.drift           r,
  /drift/ntp.drift.TEMP                  rwl,
  /drift/ntp.drift                       rwl,
}
```

Automated Workflow




```
/usr/sbin/ntpd {
  #include <abstractions/base>
  #include <abstractions/nameservice>
  capability ipc_lock,
  capability net_bind_service,
  capability sys_time,
  capability sys_chroot,
  capability setuid,
  /etc/ntp.conf                    r,
  /etc/ntp/drift*                  rwl,
  /etc/ntp/keys                    r,
  /etc/ntp/step-tickers            r,
  /tmp/ntp*                        rwl,
  /usr/sbin/ntpd                   rix,
  /var/log/ntp                     w,
  /var/log/ntp.log                 w,
  /var/run/ntpd.pid                w,
```

Native Unix Syntax, Semantics

AppArmor access controls reflect classic Unix permission patterns

- Complements Unix permissions rather than overlaying a new paradigm

Regular expressions in AppArmor rules

- `/dev/{,u}random` matches `/dev/random` and `/dev/urandom`
- `/lib/ld-*.so*` matches most of the libraries in /lib
- `/home/*/.plan` matches everyone's .plan file
- `/home/*/public_html/**` matches everyone's public HTML directory tree

Profile Building Blocks

A set of “foundation class” rules that can be #include'd in your profiles

- base: needed by nearly all programs
- authentication: program will authenticate users
- console: program interacts with TTY consoles
- kerberos: uses Kerberos cryptography
- nameservice: program needs to look up domain names
- wutmp: program updates user login logs

Includes Default Set of Policies

/etc/apparmor.d
(default loaded)

- netstat
- ping
- klogd
- syslog
- ldd
- squid
- traceroute
- identd
- mdnsd
- named
- nscd
- ntpd

/etc/apparmor/extras
(not loaded, but available)

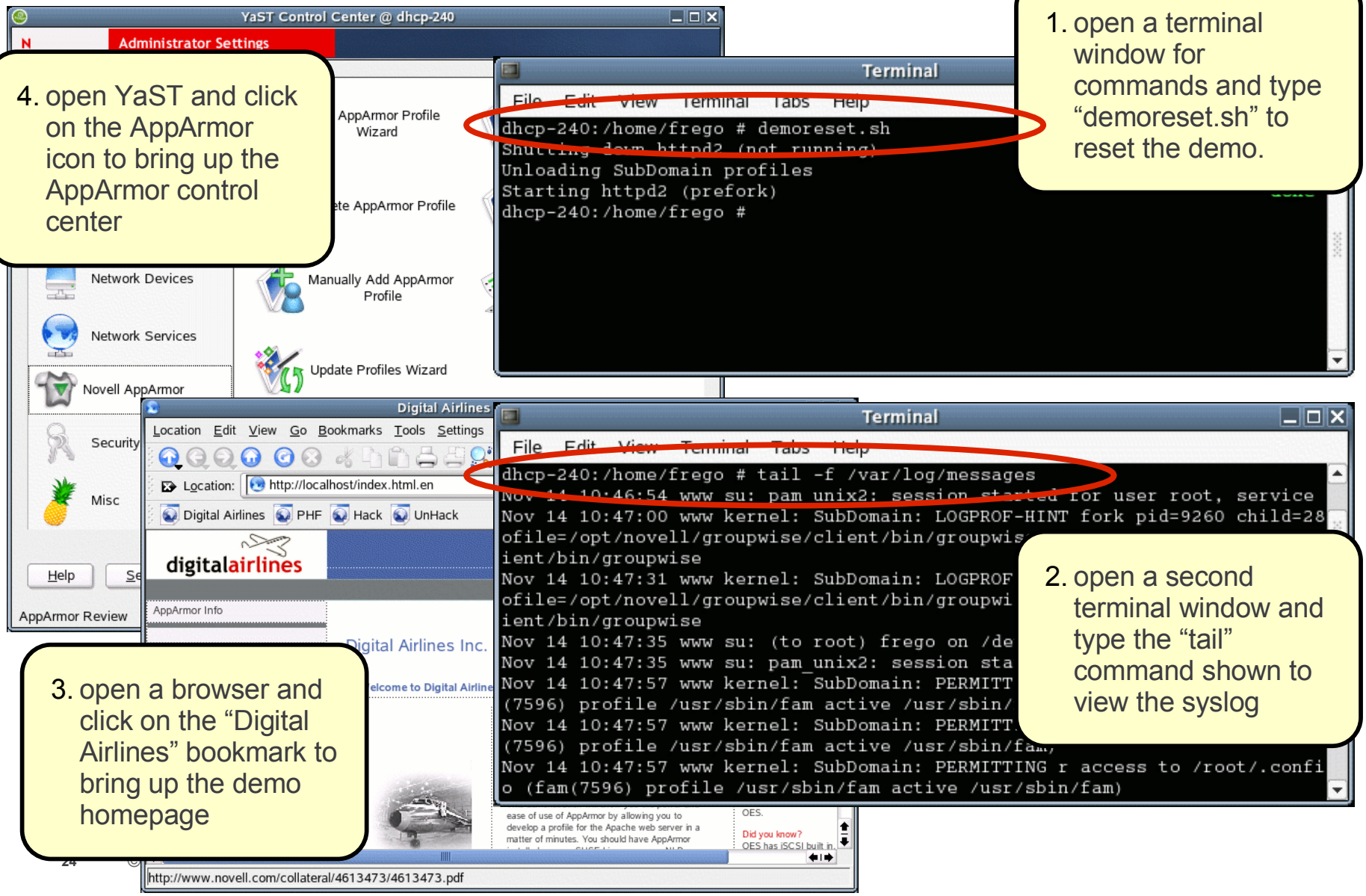
- firefox
- opera
- evolution
- gaim
- realplay
- postfix
- acroread
- mysqld
- ethereal
- postfix
- sendmail
- many more...

AppArmor Demo

Apache Profiling

1. Local Apache web server running vulnerable PHF script
2. Exploit PHF vulnerability; deface web page
3. Develop profiles for Apache and PHF app
4. Try hack again; hack fails

The Setup



1. open a terminal window for commands and type “demoreset.sh” to reset the demo.

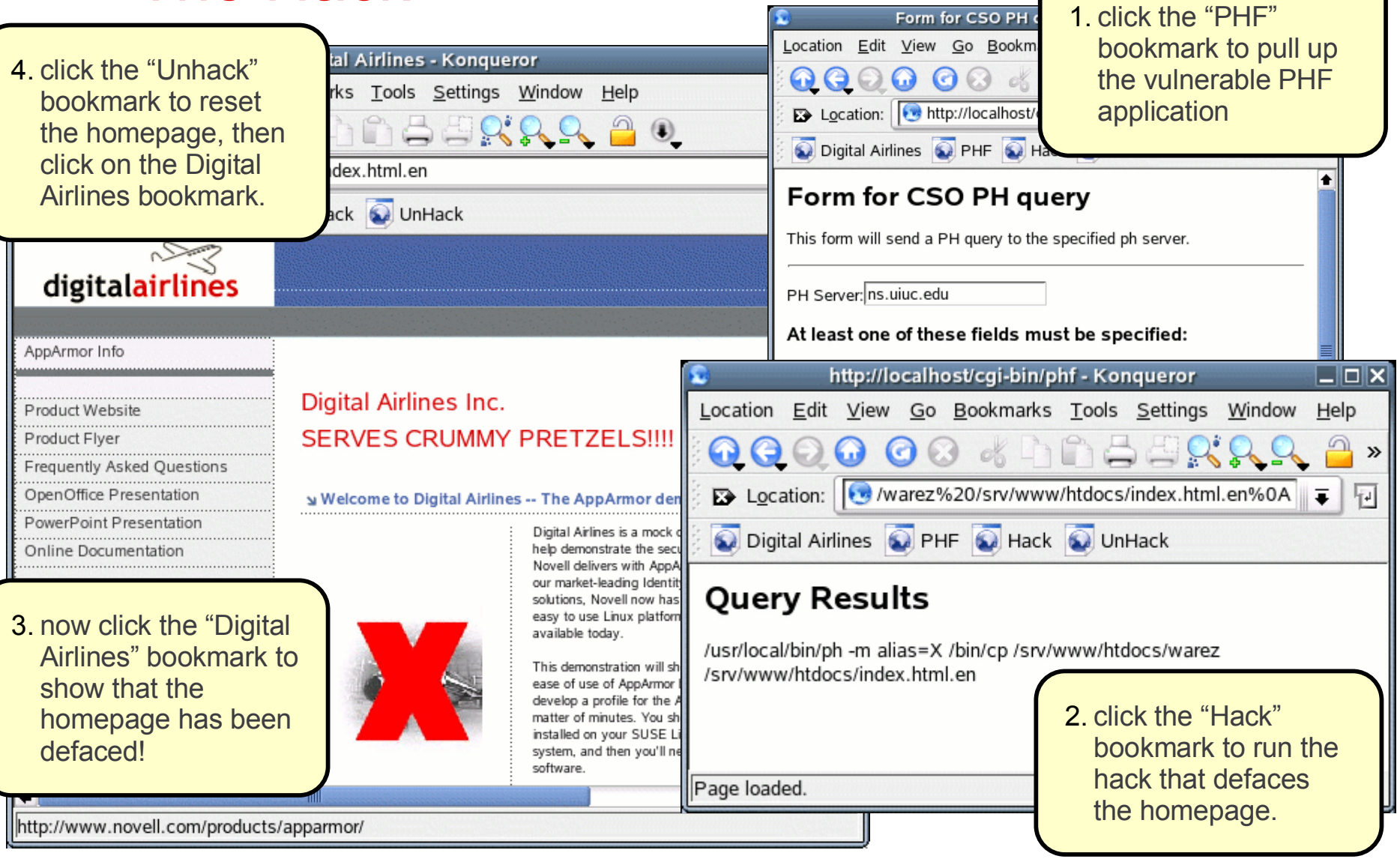
2. open a second terminal window and type the “tail” command shown to view the syslog

3. open a browser and click on the “Digital Airlines” bookmark to bring up the demo homepage

4. open YaST and click on the AppArmor icon to bring up the AppArmor control center

The Hack

4. click the “Unhack” bookmark to reset the homepage, then click on the Digital Airlines bookmark.

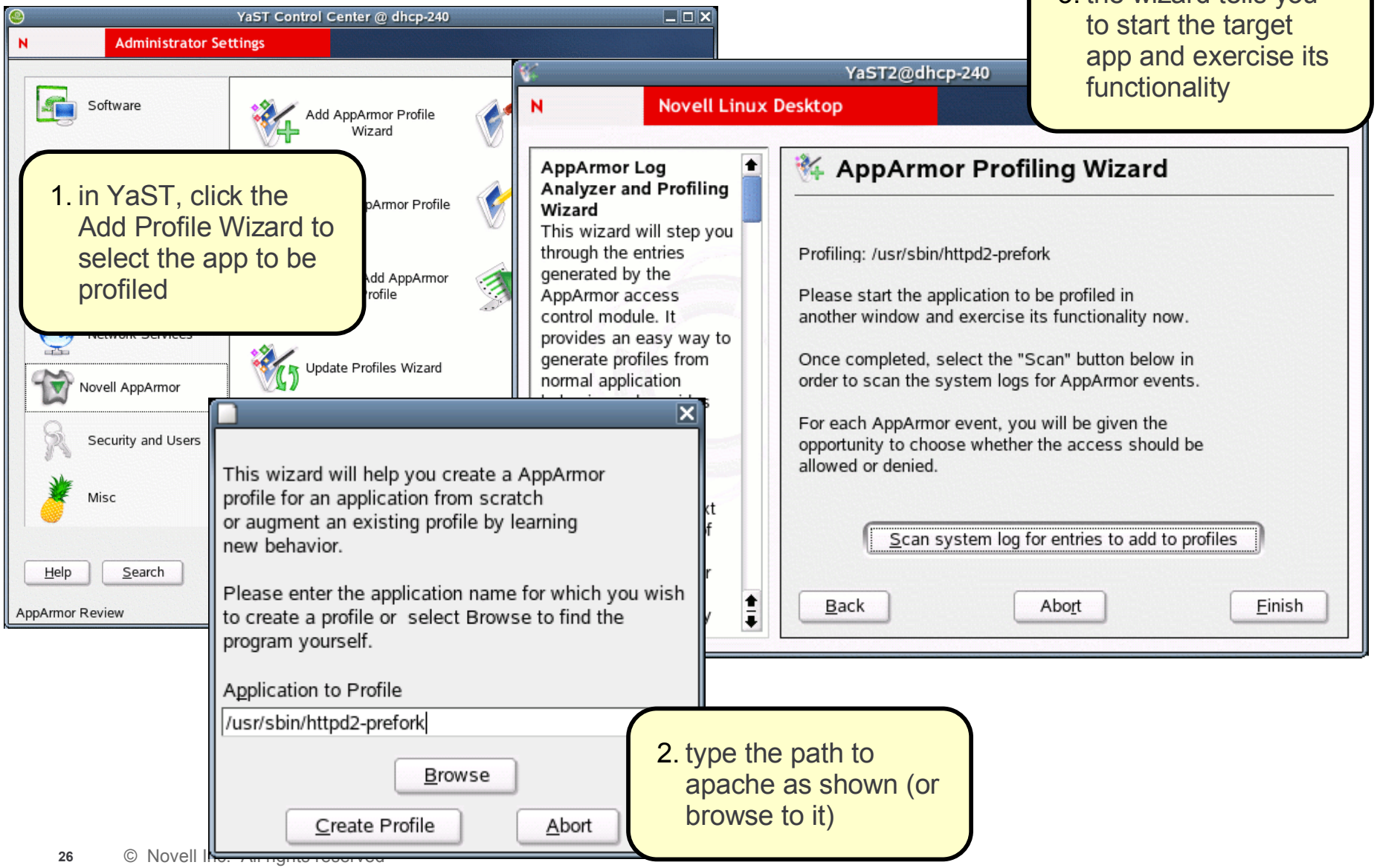


1. click the “PHF” bookmark to pull up the vulnerable PHF application

2. click the “Hack” bookmark to run the hack that defaces the homepage.

3. now click the “Digital Airlines” bookmark to show that the homepage has been defaced!

Choosing the Application

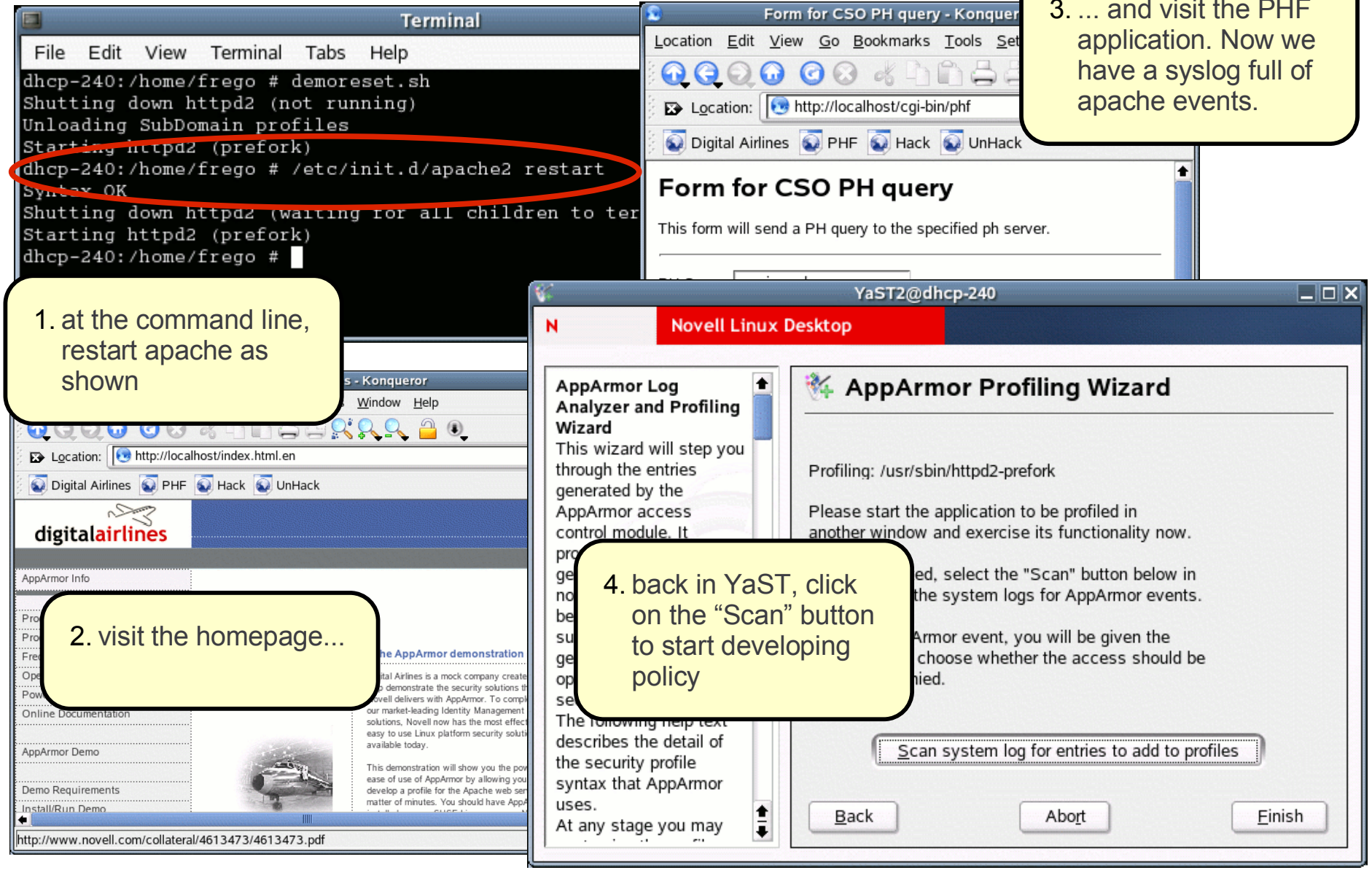


1. in YaST, click the Add Profile Wizard to select the app to be profiled

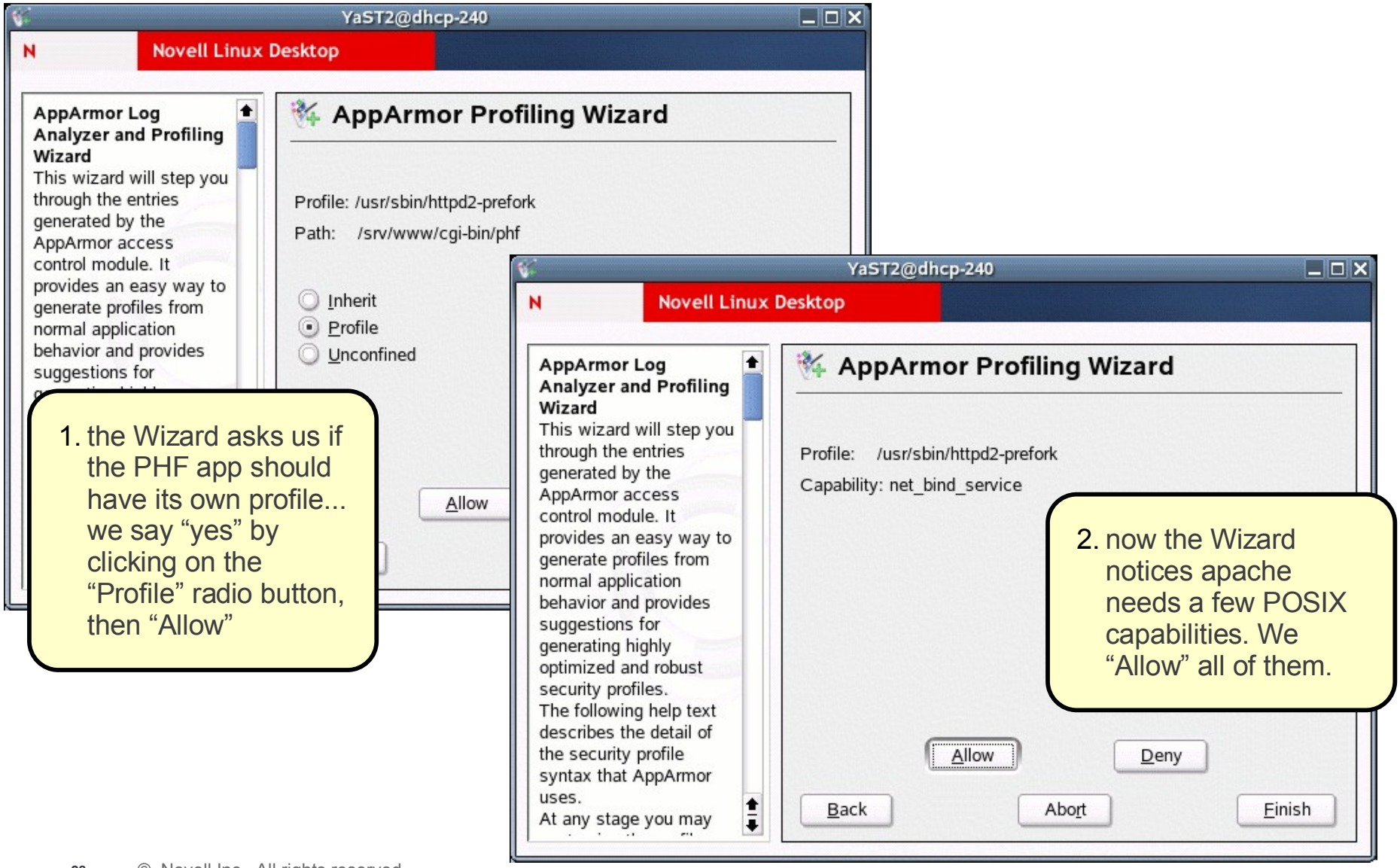
2. type the path to apache as shown (or browse to it)

3. the wizard tells you to start the target app and exercise its functionality

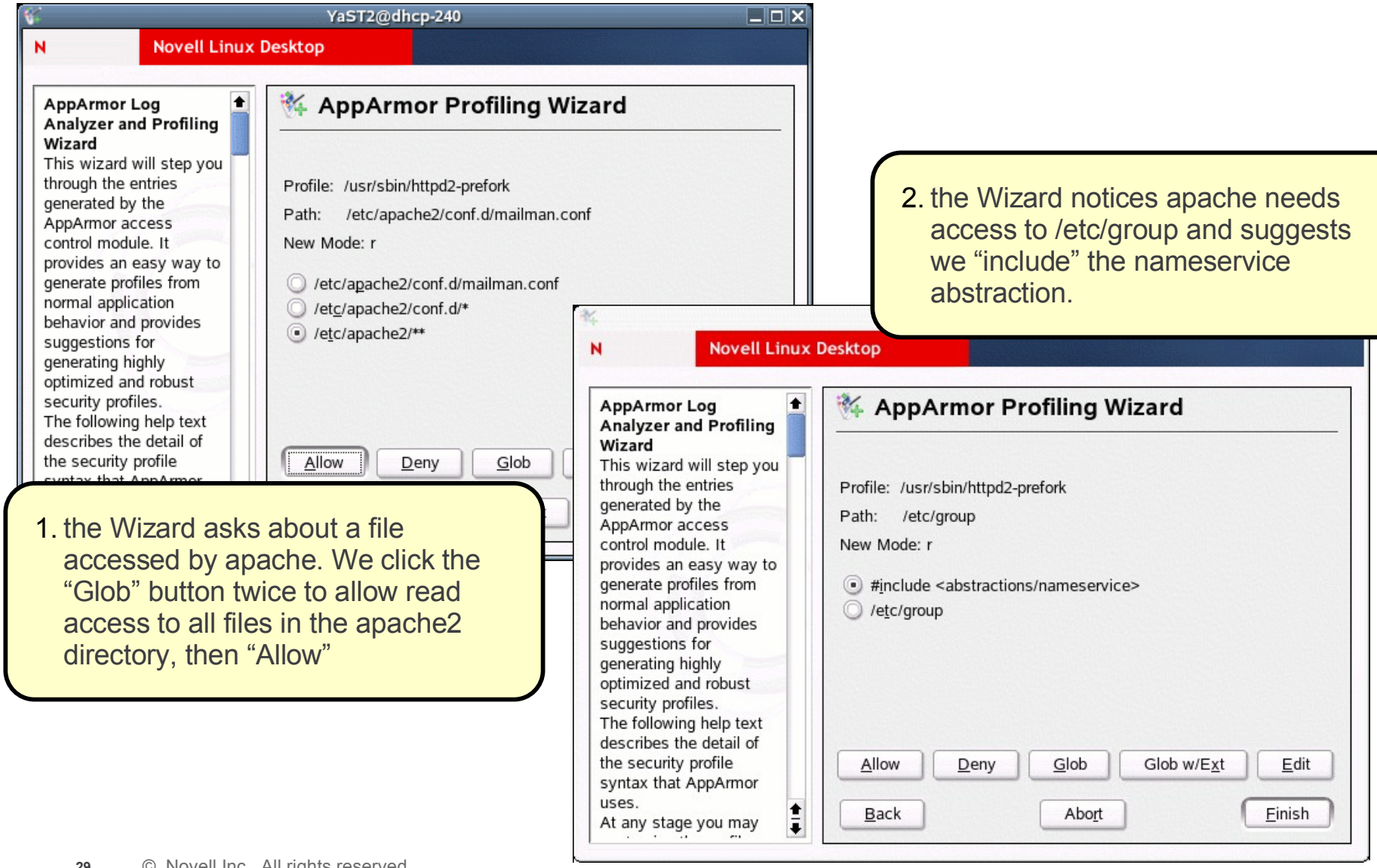
Exercising Apache



Creating AppArmor Policy



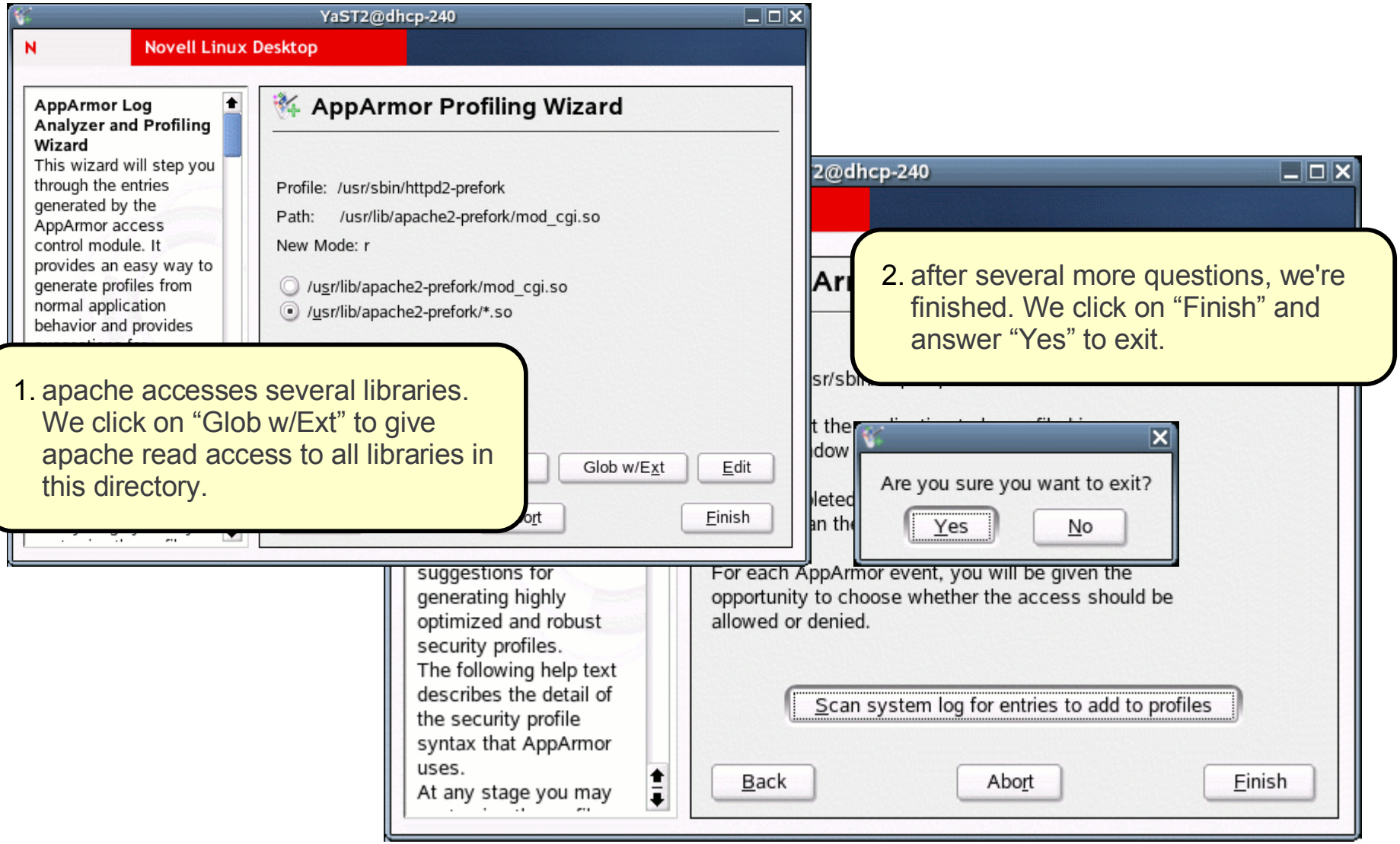
Creating AppArmor Policy 2



1. the Wizard asks about a file accessed by apache. We click the “Glob” button twice to allow read access to all files in the apache2 directory, then “Allow”

2. the Wizard notices apache needs access to /etc/group and suggests we “include” the nameservice abstraction.

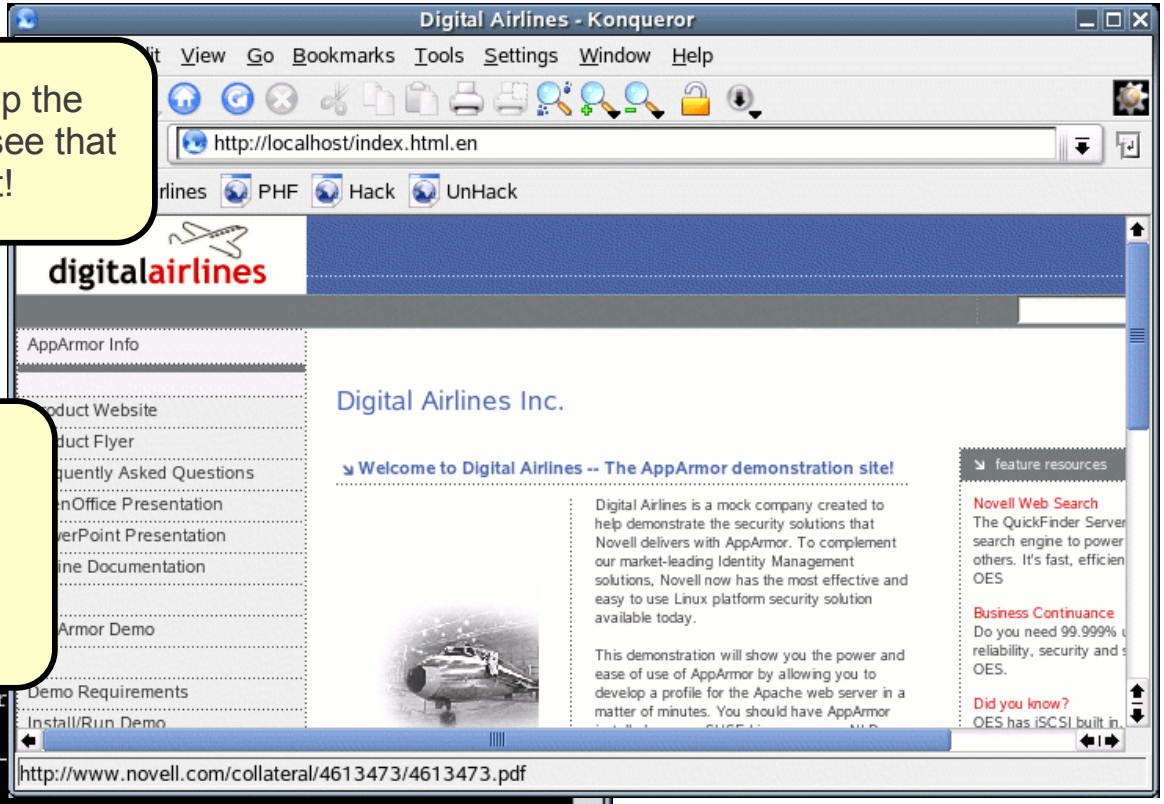
Creating Apache Policy 3

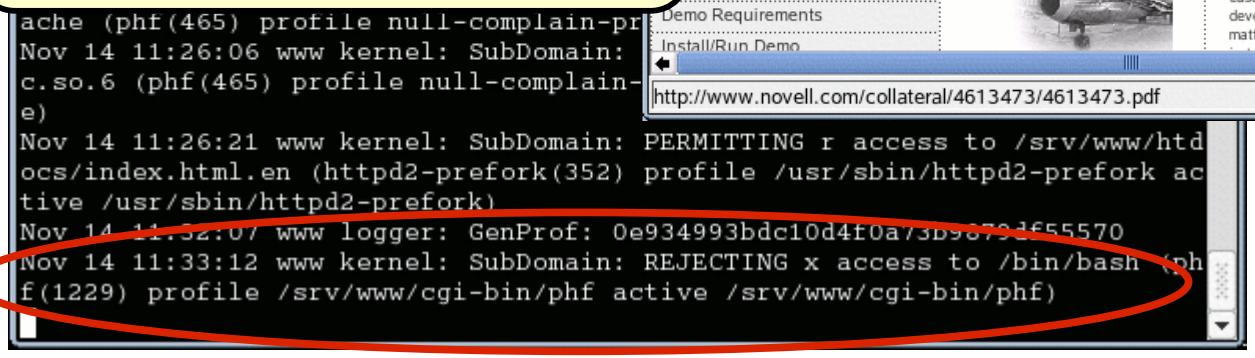


Blocking the Attack

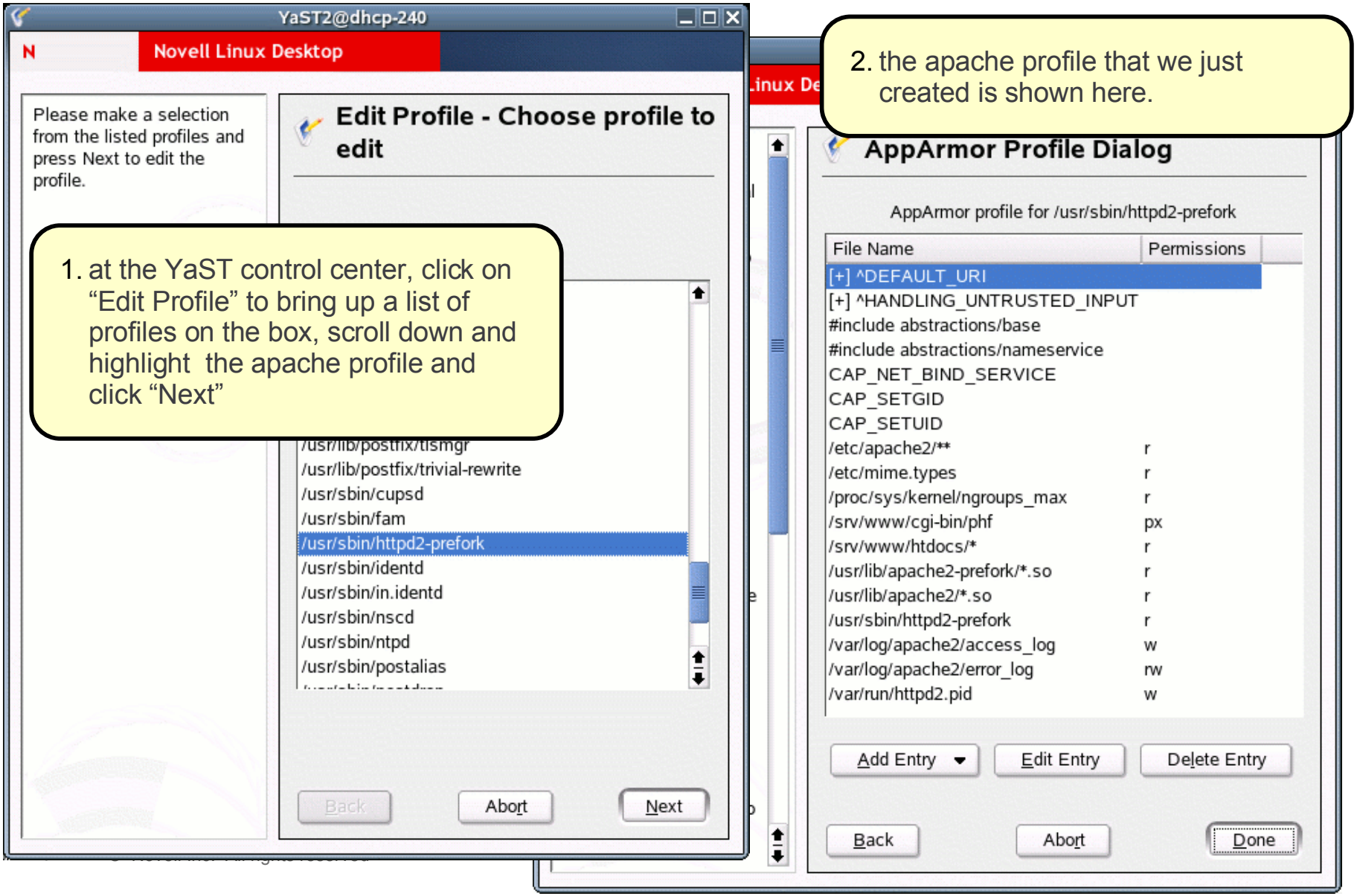
1. back at our website, we pull up the homepage, try the hack and see that the home page remains intact!

2. looking at the syslog, we see a “REJECT” entry telling us an attempted attack via the phf application was blocked by the newly created AppArmor profiles.

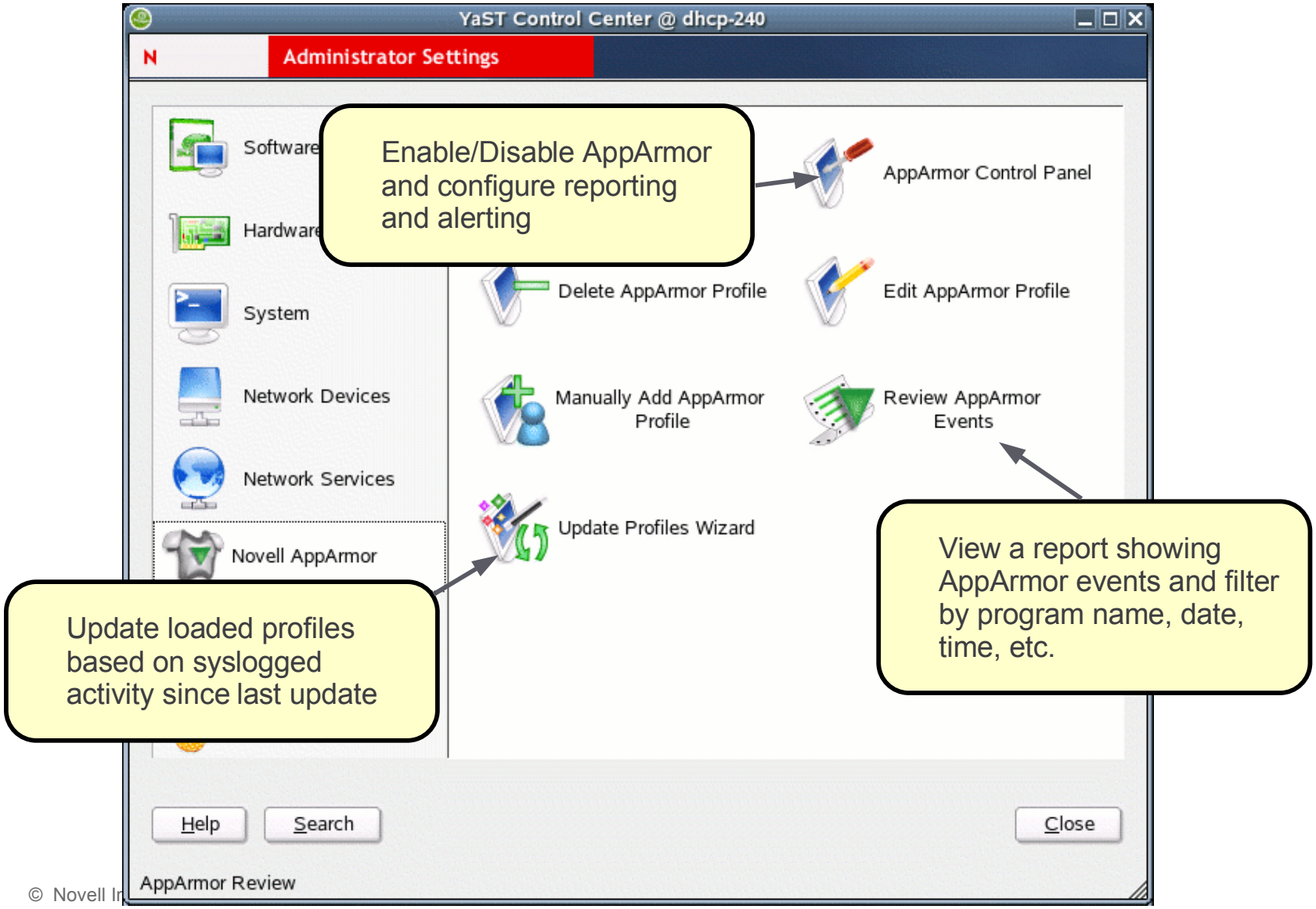




Reviewing our Apache Policy



What Else Can I Do?



Sub-process Confinement

Apache mod_perl and mod_php scripts

- Apache mod_apparmor applies new protection before interpreting scripts
- If a specific profile for that scrpt exists, it is used
- If no specific profile exists, then a default script profile is used
- Impact: don't need to run all CGIs with the full privilege of Apache just to get mod_perl efficiency
- The only known way to defend PHP code

Login Authentication

- Add a similar module to PAM: pam_armor
- Pre-authentication, sshd and logind are in a restrictive profile
- Post-authentication, can transition to per-user profile

YaST Integration

Command-line Interface

There is also a command-line interface

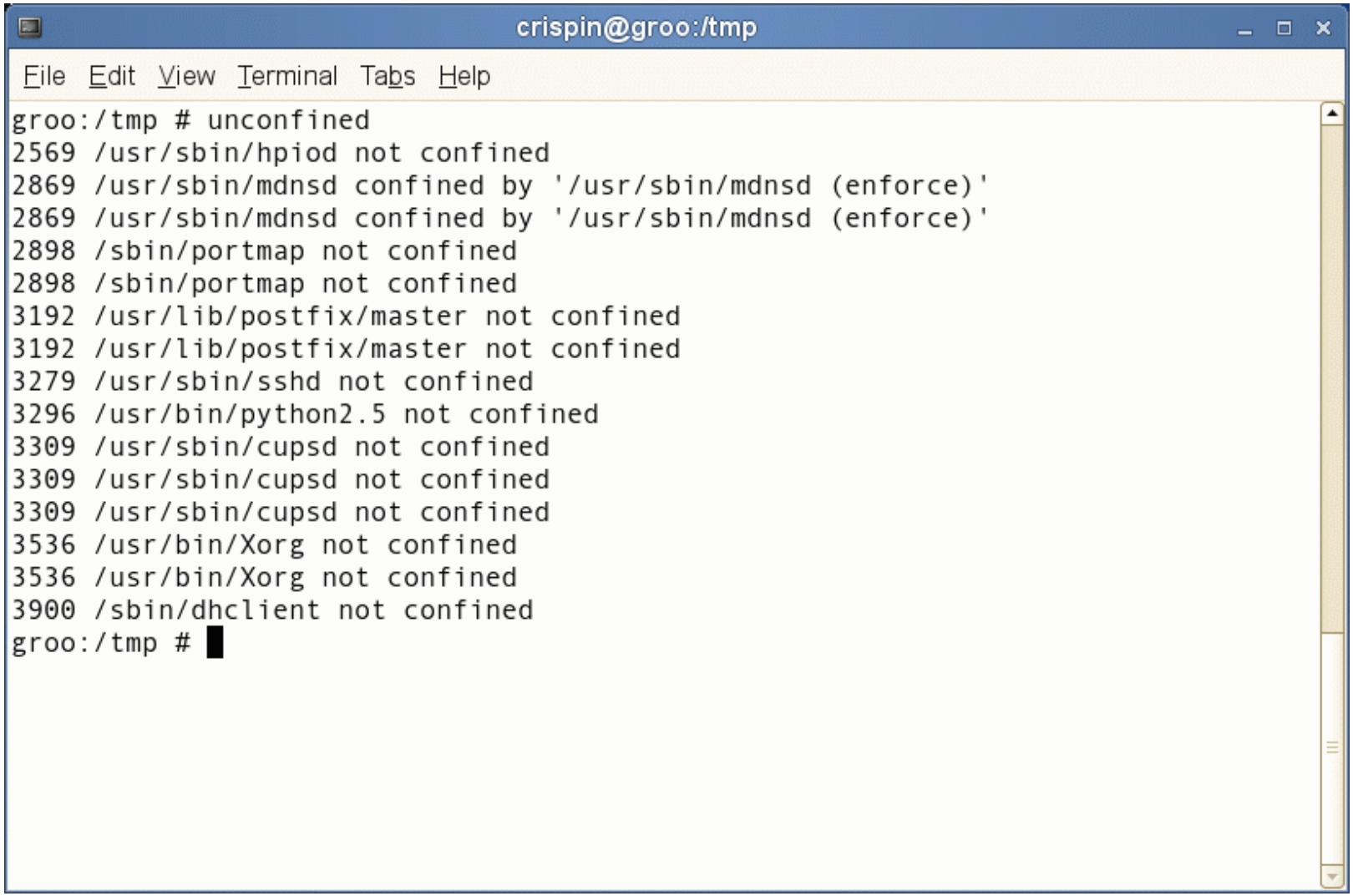
- for those of us allergic to mice :-)

GAIM Profile
Console Tools

- Create the profile template
  - cd /opt/gnome/bin
  - genprof gaim
- Exercise GAIM
  - start, chat, stop
- Create profile entries
  - [S]can log for profile entries
  - [F]inish (GAIM profile is loaded)
- View profile
  - vim opt.gnome.bin.gaim
  - syntax on
  - set syntax=subdomain

Makes it safe to talk to strangers

Network-secure a System



Network-secure a System

1. Pick an unconfined service from the list
2. Confine it the way we confined Apache and GAIM
3. Continue until all open ports lead to AppArmor profiles

Result:

- There is no way onto the machine except through an AppArmor profile
- AppArmor policy completely controls network access to the machine
- Nowhere *near* having profiled all software on the machine

Best Uses For AppArmor

Best Targets for AppArmor

Any Company whose networked servers are running mission critical applications

Any organization with a high cost associated with compromised data

Any organization faced with regulatory compliance

...

Any Linux application is exposed to attack and that matters :-)

Best Targets for AppArmor

Networked Servers

- Isolate all programs interacting with outside world
- Auto-scan tool finds applications that should be profiled
- Profiles represent your total exposure – auditable policy

Business Applications

- Complex, not easily auditable for security
- May be closed source
- Prevents attacks on one component from spreading to other components or systems

Corporate Desktop

- Profiles for desktop applications that process external data
- Separates these programs from other applications/data on the system
- Protects high-risk programs

POS Terminals, Kiosks

- Isolate all programs interacting with outside world
- Comprehensive profile set defined for specific uses
- Limits misuse of machines
- AppArmor profiles for user session and executable apps

So What Happened at CtF?

2002

- Target was Red Hat, easy to port to Immunix
- Too focused on Immunix, not enough on the game
- Delayed launching any server until we had it running on Immunix
- Placed 2nd not bad for first try

2003: Target OpenBSD

- Target was OpenBSD, took longer to port
- SQL injection attacks, AppArmor does not stop them
- Placed 3rd hmmm ...

So What Happened at CtF?

2004:

- Target Windows
- A weekend is not enough time to port 5 applications from Windows to Linux under fire :-)
- Placed 4th this trend does not look good

2005:

- Kenshoto takes over game from Ghettohackers
- Target is now under Kenshoto's control, so no more OS defensive techniques
- CtF game now focused on binary code reverse engineering

... 2007 0tB/OtB brings focus back to OS

Comparisons

Application Least Privilege for Linux

SELinux

Type Enforcement

- Assign users or programs to Domains
- Label files with Types
- Write policy in terms of which Domains can access which Types

AppArmor

Pathnames

- Name a program by path
- When it runs, it can only access the files specified by pathname
- Generalize pathnames with shell syntax wild cards

Label Splitting: SELinux

Think of SELinux as Post-it Note™ security

- Label files & programs with colored stickers
- Policy decides which colors can play together

A single label in SELinux is an equivalence class

- All files with that label are treated identically by security policy

A **human** has to decide which files should have the same label, and which files need a different label

When you get it wrong, must split the label

- Relabel all affected files
- Revise all polices that reference that label

AppArmor

AppArmor uses explicit pathnames and regular expressions to achieve the same thing

A profile rule of '/srv/www/htdoc/**.html r' is an equivalence class, with 2 differences

- The class is evaluated at access time: new files are checked against policy
- The class is local to a single profile: don't need to re-label the world to be able to distinguish 2 files that some *other* profile treats as the same

Network Storage

SELinux can only do all/nothing access control for NFS-mounted volumes

- SELinux depends on labels, which are stored in extended attributes, which are not supported in NFS2 or NFS3
- Applies a single label to the mount point
- Policies either grant or deny access to the **entire** NFS volume

AppArmor does not use extended attributes

- Can write fine-grained profiles that grant access to individual files that reside on NFS volumes

AppArmor vs. SELinux: Creating Policy

SELinux audit2allow

1. Create a file at $SELINUX_SRC/domains/program/foo.te.
2. Put the daemon domain macro call in the file.
3. Create the file contexts file.
4. Put the first list of file contexts in file.fc.
5. Load the new policy with make load.
6. Label the foo files.
7. Start the daemon, service foo start.
8. Examine your audit log for denial messages.
9. Familiarize yourself with the errors the daemon is generating.
10. Use audit2allow to start the first round of policy rules
11. Look to see if the `foo_t` domain tries to create a network socket
12. Continue to iterate through the basic steps to generate all the rules you need.
13. If the domain tries to access `port_t`, which relates to `tclass=tcp_socket` or `tclass=udp_socket` in the AVC log message, you need to determine what port number foo needs to use.
14. Iterate through the remaining AVC denials. When they are resolved with new policy, you can configure the unique port requirements for the `foo_t` domain.
15. With the daemon started, determine which port foo is using.
16. Remove the generic port_t rule, replacing it with a specific rule for a new port type based on the foo_t domain.

AppArmor

1. Open YaST Control Center
2. Run Server Analyzer to determine which programs to profile
3. Run the Profile Wizard to generate a profile template
4. Run the application through normal operation
5. Run the interactive optimizer to synthesize log events into a profile

AppArmor vs. SELinux:
Compare Resulting Policy

- SELinux

```
################################
#
# Rules for the ftpd_t domain
#
type ftp_port_t, port_type;
type ftp_data_port_t, port_type;
daemon_domain(ftpd, `, auth_chkpwd')
type etc_ftpd_t, file_type, sysadmfile;

can_network(ftpd_t)
can_ypbind(ftpd_t)
allow ftpd_t self:unix_dgram_socket create_socket_perms;
allow ftpd_t self:unix_stream_socket create_socket_perms;
allow ftpd_t self:process {getcap setcap};
allow ftpd_t self:fifo_file rw_file_perms;

allow ftpd_t bin_t:dir search;
can_exec(ftpd_t, bin_t)
allow ftpd_t { sysctl_t sysctl_kernel_t }:dir search;
allow ftpd_t sysctl_kernel_t:file { getattr read };
allow ftpd_t urandom_device_t:chr_file { getattr read };

ifdef(`crond.te', `
system_crond_entry(ftpd_exec_t, ftpd_t)
can_exec(ftpd_t, { sbin_t shell_exec_t })
')

allow ftpd_t ftp_data_port_t:tcp_socket name_bind;

ifdef(`ftpd_daemon', `
define(`ftpd_is_daemon', `')
') dnl end ftpd_daemon
ifdef(`ftpd_is_daemon', `
rw_dir_create_file(ftpd_t, var_lock_t)
allow ftpd_t ftp_port_t:tcp_socket name_bind;
allow ftpd_t self:unix_dgram_socket { sendto };
can_tcp_connect(userdomain, ftpd_t)
', `
ifdef(`inetd.te', `
domain_auto_trans(inetd_t, ftpd_exec_t, ftpd_t)
ifdef(`tcpd.te', `domain_auto_trans(tcpd_t, ftpd_exec_t, ftpd_t)')

# Use sockets inherited from inetd.
allow ftpd_t inetd_t:fd use;
allow ftpd_t inetd_t:tcp_socket rw_stream_socket_perms;

# Send SIGCHLD to inetd on death.
allow ftpd_t inetd_t:process sigchld;
') dnl end inetd.te
')dnl end (else) ftp_is_daemon
ifdef(`ftp_shm', `
allow ftpd_t tmpfs_t:file { read write };
allow ftpd_t { tmpfs_t initrc_t }:shm { read write unix_read unix_write associate };
')

# Use capabilities.
allow ftpd_t ftpd_t:capability { net_bind_service setuid setgid fowner fsetid chown sys_resource sys_chroot };

# Append to /var/log/wtmp.
allow ftpd_t wtmp_t:file { getattr append };

# allow access to /home
allow ftpd_t home_root_t:dir { getattr search };

# Create and modify /var/log/xferlog.
type xferlog_t, file_type, sysadmfile, logfile;
file_type_auto_trans(ftpd_t, var_log_t, xferlog_t, file)
# Execute /bin/ls (can comment this out for proftpd)
# also may need rules to allow tar etc...
can_exec(ftpd_t, ls_exec_t)

allow { ftpd_t initrc_t } etc_ftpd_t:file r_file_perms;
allow ftpd_t { etc_t resolv_conf_t etc_runtime_t }:file { getattr read };
allow ftpd_t proc_t:file { getattr read };


')dnl end if ftp_home_dir
```

- AppArmor

```
/usr/sbin/in.ftpd {
  #include <immunix-standard/base>
  #include <immunix-standard/nameservice>
  #include <immunix-standard/authentication>
  #include <user-custom/ftpd>
  /                                 r,
  /dev/urandom                      r,
  /etc/fstab                        r,
  /etc/ftpaccess                    r,
  /etc/ftpconversions               r,
  /etc/ftphosts                     r,
  /etc/ftpusers                     r,
  /etc/shells                       r,
  /usr/sbin/in.ftpd                 r,
  /usr/share/ssl/certs/ca-bundle.crt        r,
  /usr/share/ssl/certs/ftpd-rsa.pem         r,
  /usr/share/ssl/private/ftpd-rsa-key.pem   r,
  /usr/share/ssl/.rnd               w,
  /var/log/xferlog                  w,
  /var/run                          wr,
  /var/run/ftp.{pids,rips}-all      wr,
}
```

AppArmor profile for the *same program* is about 4x smaller

AppArmor vs. SELinux:
Compare Resulting Policy

- SELinux

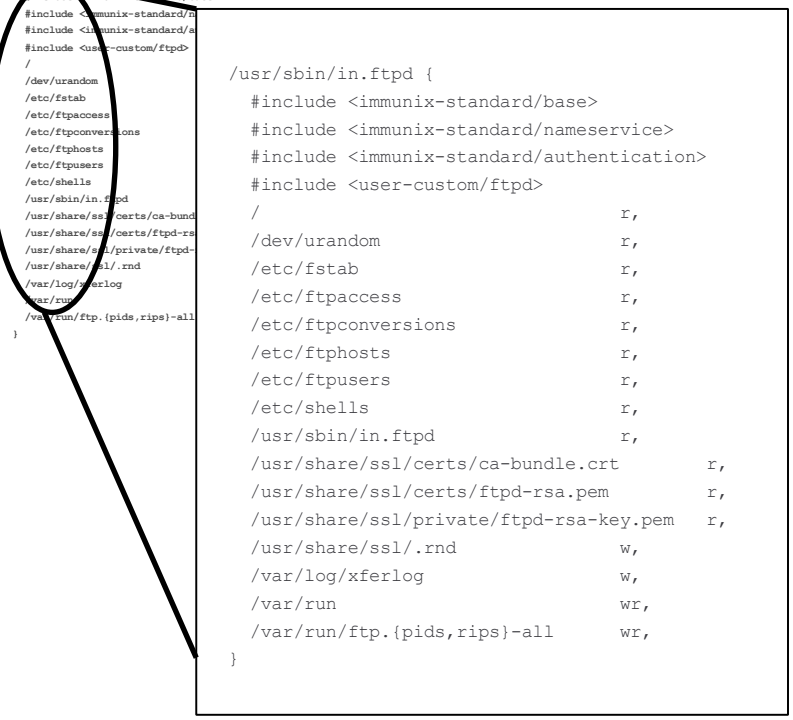
```
.
ifdef(`ftpd_daemon', `
define(`ftpd_is_daemon', `')
') dnl end ftpd_daemon
ifdef(`ftpd_is_daemon', `
rw_dir_create_file(ftpd_t, var_lock_t)
allow ftpd_t ftp_port_t:tcp_socket name_bind;
allow ftpd_t self:unix_dgram_socket { sendto };
can_tcp_connect(userdomain, ftpd_t)
', `
ifdef(`inetd.te', `
domain_auto_trans(inetd_t, ftpd_exec_t, ftpd_t)
ifdef(`tcpd.te', `domain_auto_trans(tcpd_t,
    ftpd_exec_t, ftpd_t)')

# Use sockets inherited from inetd.
allow ftpd_t inetd_t:fd use;
allow ftpd_t inetd_t:tcp_socket
    rw_stream_socket_perms;

# Send SIGCHLD to inetd on death.
allow ftpd_t inetd_t:process sigchld;
') dnl end inetd.te
')dnl end (else) ftp_is_daemon
ifdef(`ftp_shm', `
allow ftpd_t tmpfs_t:file { read write };
allow ftpd_t { tmpfs_t initrc_t }:shm { read
    write unix_read unix_write associate };
')
.
.
```

SELinux uses a custom programming language to specify hard-to-manage rules

- AppArmor



```
/usr/sbin/in.ftpd {
  #include <immunix-standard/base>
  #include <immunix-standard/nameservice>
  #include <immunix-standard/authentication>
  #include <user-custom/ftpd>
  /                                    r,
  /dev/urandom                         r,
  /etc/fstab                           r,
  /etc/ftpaccess                       r,
  /etc/ftpconversions                  r,
  /etc/ftphosts                        r,
  /etc/ftpusers                        r,
  /etc/shells                          r,
  /usr/sbin/in.ftpd                    r,
  /usr/share/ssl/certs/ca-bundle.crt       r,
  /usr/share/ssl/certs/ftpd-rsa.pem        r,
  /usr/share/ssl/private/ftpd-rsa-key.pem  r,
  /usr/share/ssl/.rnd                  w,
  /var/log/xferlog                     w,
  /var/run                             wr,
  /var/run/ftp.{pids,rips}-all         wr,
}
```

Classical Linux syntax with read/write/execute permissions: No new jargon

SELinux New GUI Tools

- Advanced GUIs for enabling and disabling chunks of pre-written policies
  - No help for authoring new policies
- Works great for software that someone else has already profiled for you
  - Problematic for your in-house and 3rd party software
- AppArmor:
  - It's not the GUI, it is the fundamental model

AppArmor Roadmap

AppArmor Near Term Development

Network Access Control – TCP/UDP based network access control per process

Profile Merge Tool – allows two profiles to be merged into a single profile consisting of union set of both

Profile Sharing – tools and portal for community sharing of AppArmor profiles

Tomcat Support – AppArmor containment for Java servlets

PAM change_hat – strengthens security of AppArmor's role-based shell functionality for applications that use PAM (e.g., sshd, gdm, ftp)

CIM Providers – Standards based CIM instrumentation for Reporting, Alerting, Profile State

AppArmor Future Development

DB Armor – access controls for database tables and files

Default Policy – system level list of resources that can *only* be accesses through an AppArmor profile

DBUS Event Advertising – report security events via DBUS

DBUS / HAL Event Mediation – containment for hardware abstraction layer

IPC Mediation – mediate inter-process communication

Enterprise Management – integration with Novell enterprise management system

Profile Lint – tool for analyzing profiles for dangerous rules

Resource Limits Mediation

Centralized Profile Development

Availability

AppArmor bundled with:

- SLES10
- SLED10
- openSUSE 10.1, 10.2 ...

AppArmor is open source: GPL

- http://opensuse.org/AppArmor
- Mailing lists: apparmor-announce, apparmor-general, apparmor-dev
- IRC irc.oftc.net/#apparmor

AppArmor for Ubuntu

AppArmor ported to Ubuntu by Magnus Runesson

- http://www.linuxalert.org/ubuntu/apparmor/

AppArmor in Universe for Feisty Fawn

AppArmor going into Main for Gutsy Gibbon

User feedback on profiles is **very** helpful

AppArmor for Everyone

Ported to Gentoo by Mathew Snelham:

- http://sigalrm.com/apparmor/apparmor-ebuilds_2006

Debian:

- Should be easy to generate from Ubuntu port
- Need a maintainer
- AppArmor's ease of use makes it a good idea for a de facto Linux security standard

AppArmor for Debian

AppArmor has already been ported to Ubuntu by Magnus Runesson

- http://www.linuxalert.org/ubuntu/apparmor/
- In discussion for mainstream inclusion in future Ubuntu releases

and to Gentoo by Mathew Snelham

- http://sigalrm.com/apparmor/apparmor-ebuilds_2006

Debian:

- Should be easy to generate from Ubuntu port
- Need a maintainer

AppArmor for Red Hat

AppArmor has been ported to RH variants multiple times

- But the people doing the work didn't want to be public maintainers, so no public repository

Steve Beattie @ SUSE ported to RHEL5

- http://developer.novell.com/wiki/index.php/Special:Downloads/apparmor/Development_-_RHEL5_beta_2_packages/
- http://software.opensuse.org/download/home:/steve-beattie/Fedora_Extras_6/

Seeking a RH/Fedora user to maintain the package


Novell®