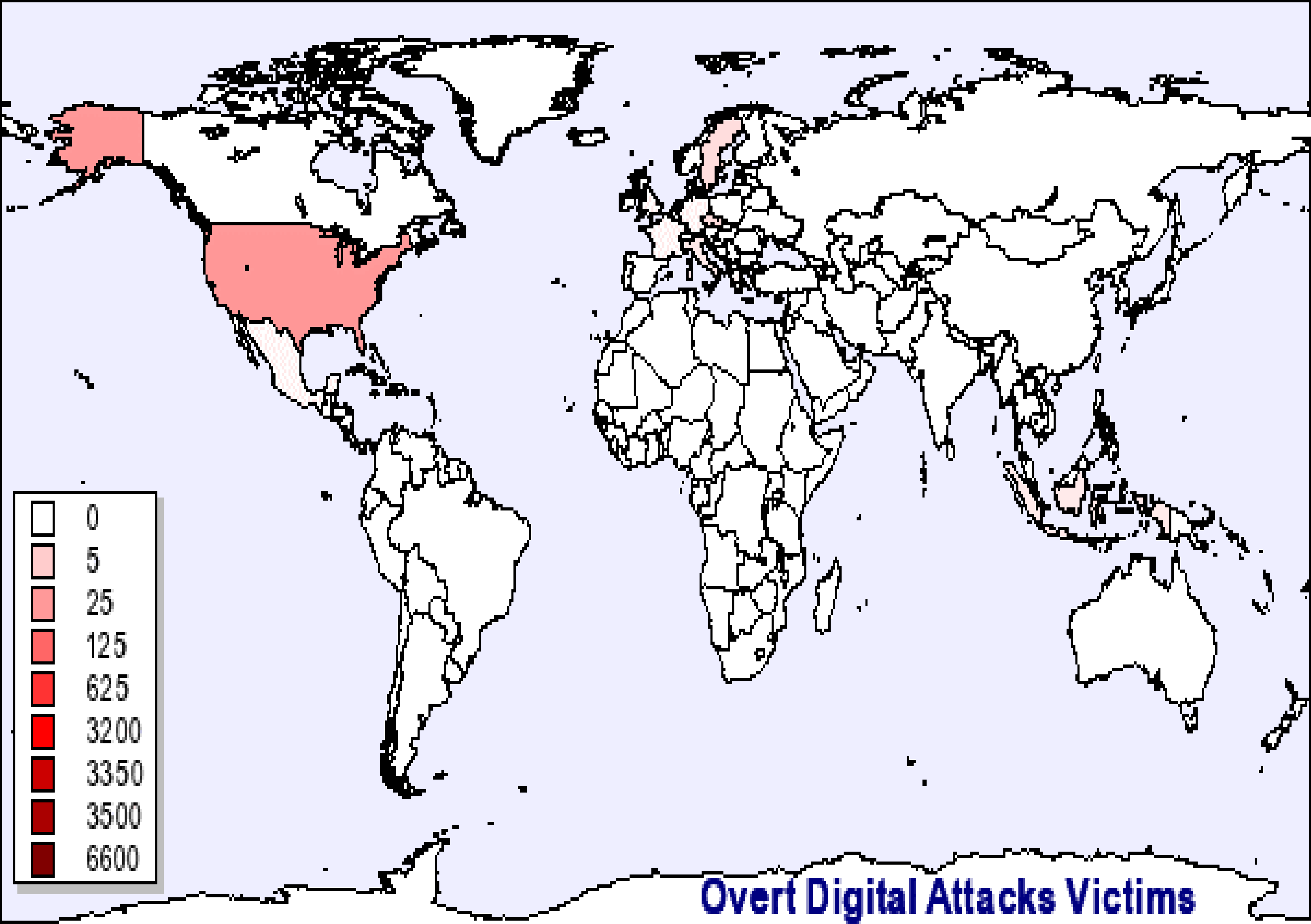
Introduction to UNIX/LINUX Security

Hu Weiwei

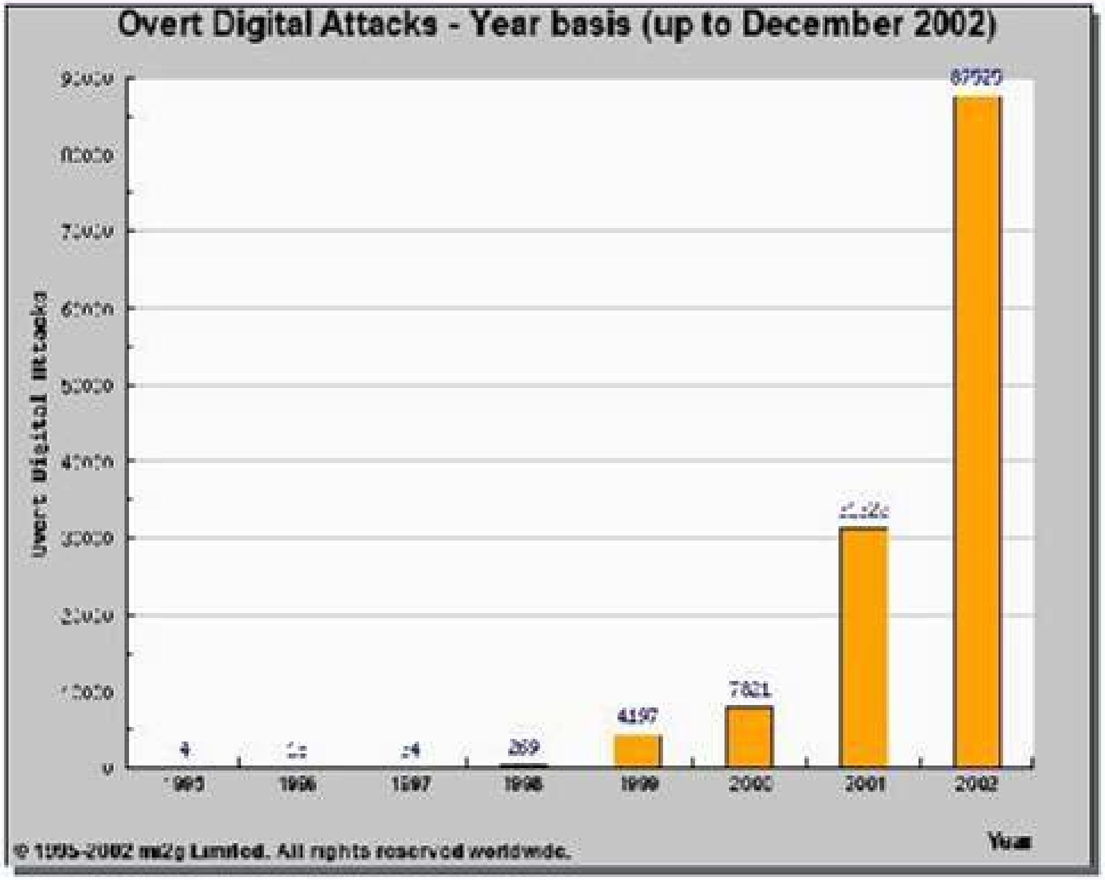
Operation System Security

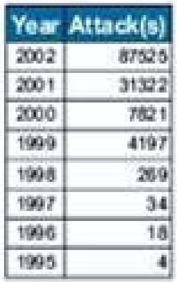
- The Security Problems in Operation Systems become more and more important
- The Security techniques improved rapidly
- The number of computer attaked rises every year



Overt Digital Attacks Victims
for 1998-01 : 51

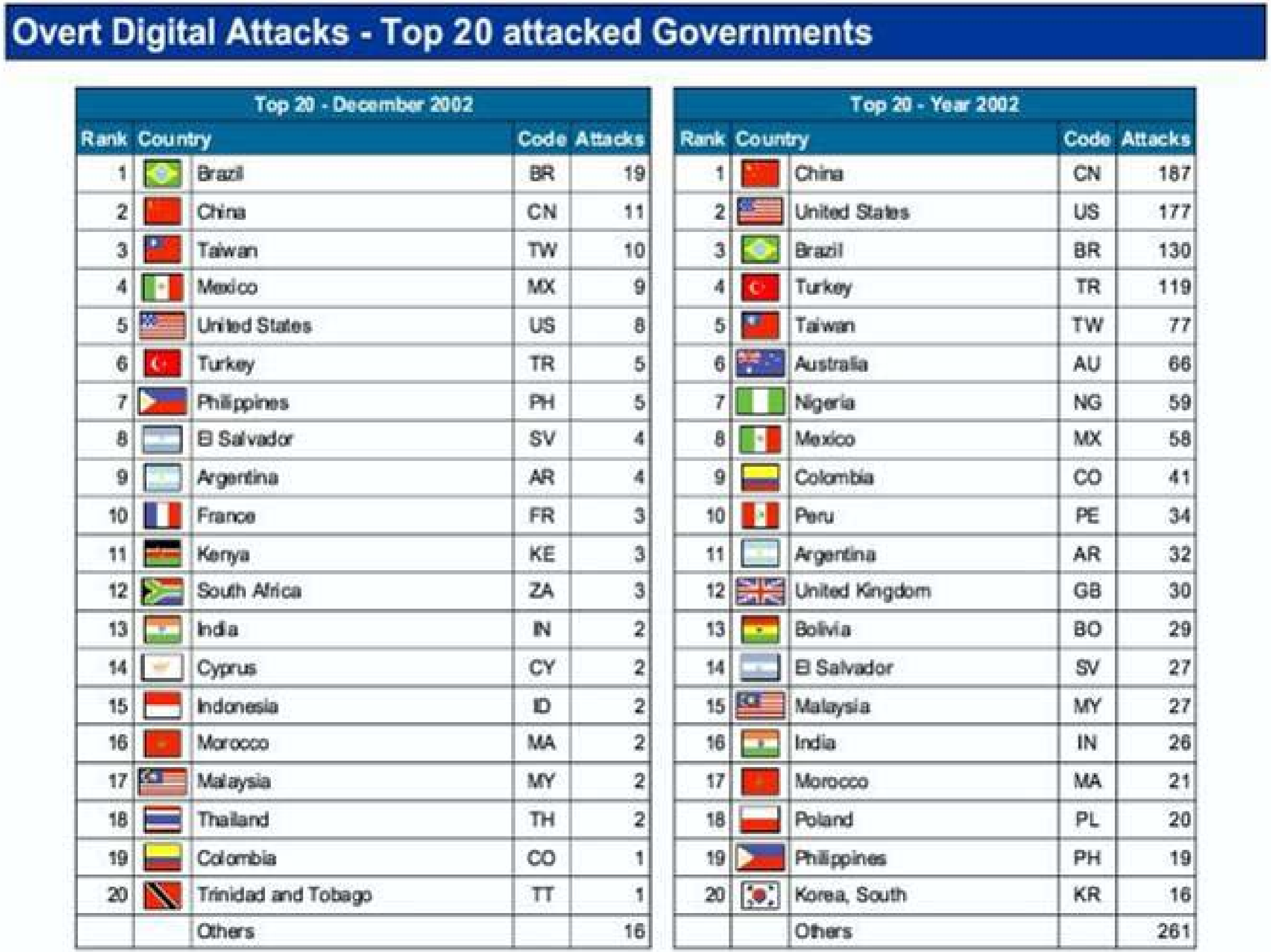
Overt Digital Attacks - Yearly trend (from 1995)





Year	Attack(s)
2002	87525
2001	31322
2000	7821
1999	4197
1998	269
1997	34
1996	18
1995	4

***Note:** the number in the table for 2002 is "to-date", whereas the value shown in the graph is a projection calculated pro-rata.*

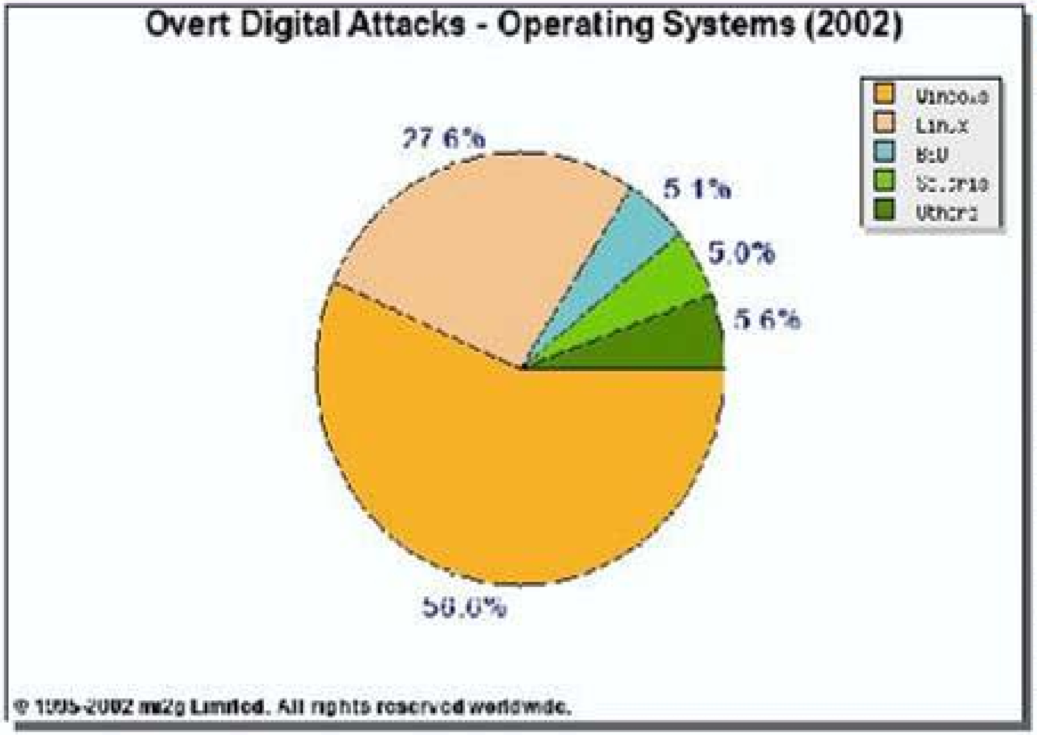


Overt Digital Attacks - Top 20 attacked Governments

Top 20 - December 2002			
Rank	Country	Code	Attacks
1	Brazil	BR	19
2	China	CN	11
3	Taiwan	TW	10
4	Mexico	MX	9
5	United States	US	8
6	Turkey	TR	5
7	Philippines	PH	5
8	El Salvador	SV	4
9	Argentina	AR	4
10	France	FR	3
11	Kenya	KE	3
12	South Africa	ZA	3
13	India	IN	2
14	Cyprus	CY	2
15	Indonesia	ID	2
16	Morocco	MA	2
17	Malaysia	MY	2
18	Thailand	TH	2
19	Colombia	CO	1
20	Trinidad and Tobago	TT	1
	Others		16

Top 20 - Year 2002			
Rank	Country	Code	Attacks
1	China	CN	187
2	United States	US	177
3	Brazil	BR	130
4	Turkey	TR	119
5	Taiwan	TW	77
6	Australia	AU	66
7	Nigeria	NG	59
8	Mexico	MX	58
9	Colombia	CO	41
10	Peru	PE	34
11	Argentina	AR	32
12	United Kingdom	GB	30
13	Bolivia	BO	29
14	El Salvador	SV	27
15	Malaysia	MY	27
16	India	IN	26
17	Morocco	MA	21
18	Poland	PL	20
19	Philippines	PH	19
20	Korea, South	KR	16
	Others		261

Operating Systems - Top attacked OS (2002)



Overt Digital Attacks - Operating Systems (2002)

Rank	Operating System	Attacks
1	Windows	49527
2	Linux	24189
3	BSD	4490
4	Solaris	4395
5	Unknown	3369
6	Unix	783
7	AIX	254
8	IRIX	193
9	SCO Unix	187
10	MacOS	79
11	HP-UX	24
12	Compaq Tru64	12
13	OS/2	11
14	Novell	6
15	Digital Unix	3
16	VM	2
17	OS/390	1

Why Do I Care?

- UNIX systems designed to be servers
- can do almost anything remotely
- Beavis and Butthead are out there
  - loss of data
  - use your machine to "attack" others
  - theft/denial of service
  - pretend they're you

Usernames and Passwords

- username and password required
- usually only password not "public"
- modern UNIX's hide encrypted password
- pick password carefully, avoid
  - dictionary words
  - names
  - simple modifications of above

Good User Habits

- change password periodically
- don't let people watch login
- lock display when unattended
- log off when leaving
- never ever ever give out password
  - even sys-admin should never need it

Superuser

- username "root"
- can do anything
- sometimes extra restrictions (remote logins)
- used for system maintenance
  - normal users can't modify system files
- **BAD** idea to login as root
  - su
  - sudo

Accessing Remote Systems

- often need to provide username/password
- potential vulnerability depends on network path connection flows through
- many connections pass plain text
  - telnet particularly bad, rlogin/ftp bad too
- SSH encrypts data on network
  - slogin for logins
  - scp for file transfer

Network Connection

- dial-up PPP less risky but slower
- DSL or Cable Modem more risky but faster
  - always a target
- ISP may act as firewall
  - simplest form stops initialization of connection flowing to your machine
  - more complex may evaluate based on net ports, source address, etc.

Network Connection

- even if only one machine on DSL/Cable Modem consider "Cable Modem Router"
  - uses NAT
  - acts as basic firewall
  - most allow configuring specific ports to pass through
  - can use many Free UNIX's as routers

Daemons

- started at boot time, run all the time
- provide services
  - SysVinit
  - at
  - bdflush
  - printing
  - mail transfer
  - accept remote logins

Daemons

- usually run as root user
- can have bugs
- Update the kernel
- Get patch

UNIX vulnerabilities

- U1 Remote Procedure Calls (RPC)
- U2 Apache Web Server
- U3 Secure Shell (SSH)
- U4 Simple Network Management Protocol (SNMP)
- U5 File Transfer Protocol (FTP)
- U6 R-Services—Trust Relationships
- U7 Line Printer Daemon (LPD)
- U8 Sendmail
- U9 BIND/DNS
- U10 General UNIX Authentication—Accounts with No Passwords or Weak Passwords

UNIX System Configuration Problems

- Weak passwords
- Accounts without passwords or default passwords
- Reusable passwords
- Use of TFTP (Trivial File Transfer Protocol) to steal password files
- Vulnerabilities in sendmail
- Old versions of FTP; misconfigured anonymous FTP

UNIX System Configuration Problems

- Misconfiguration of uucp
- Old versions of system software
- Use of setuid shell scripts

How To Determine Whether Your System Has Been Compromised

- Examine log files such as your 'last' log, process accounting, syslog, and C2 security logs for logins from unusual locations or other unusual activity
- Look everywhere on the system for unusual or hidden files (files that start with a period and are normally not shown by ls) as these can be used to hide information such as password cracking programs and password files from other systems.
- Look for setuid files (especially setuid root files) everywhere on your system. Intruders often leave setuid copies of /bin/sh around to allow them root access at a later time.
- Check your system binaries to make sure that they haven't been changed.

How To Determine Whether Your System Has Been Compromised

- Examine all the files that are run by cron and at.
- Inspect /etc/inetd.conf for unauthorized additions or changes.
- Check your system and network configuration files for unauthorized entries.
- Examine all machines on the local network when searching for signs of intrusion.
- Examine the /etc/passwd file on the system and check for any additional or modified accounts.

Protecting Your System

- starts with installation of OS
  - don't install stuff you don't need
  - new RedHat release offers "firewall" protection during install (IPCHAIN)
  - immediately create unprivileged user, use that as your normal login
  - most likely want "Workstation" type install

Protecting Your System

- check things after install
  - look at full process listing
  - slowly learn more about system and what these processes do
  - manual pages usually available
  - many Free UNIX's criticized for having too much stuff running by default

Protecting Your System

- adjust stand-alone daemons
  - different mechanisms on different platforms
    - RedHat: chkconfig command
    - FreeBSD: **/etc/defaults/rc.conf** sets various variables, override them in **/etc/rc.conf**
    - Sys-V based systems startup scripts in **/etc/rc*.d**
  - sendmail particularly bad, consider not running it or removing **–bd** command flag

Protecting Your System

- **inetd** known as "super-daemon"
  - starts up other daemons (e.g. telnet) on demand
  - config file usually **/etc/inetd.conf**
  - comment out lines you don't need
  - can send running **inetd** process HUP signal to have it re-read **/etc/inetd.conf**
  - look at tcpwrappers package for further protection

Protecting Your System

- IPCHAINS is Linux-ism enabled with new RedHat release
- blocks network ports inside kernel
- install screens refer to it as "firewall"
- if initially installed can adjust later with file **/etc/sysconfig/ipchains**