Chapter 10
Phase 4: Maintaining Access

Trojan Horses

- Software program containing a concealed malicious capability but appears to be benign, useful, or attractive to users

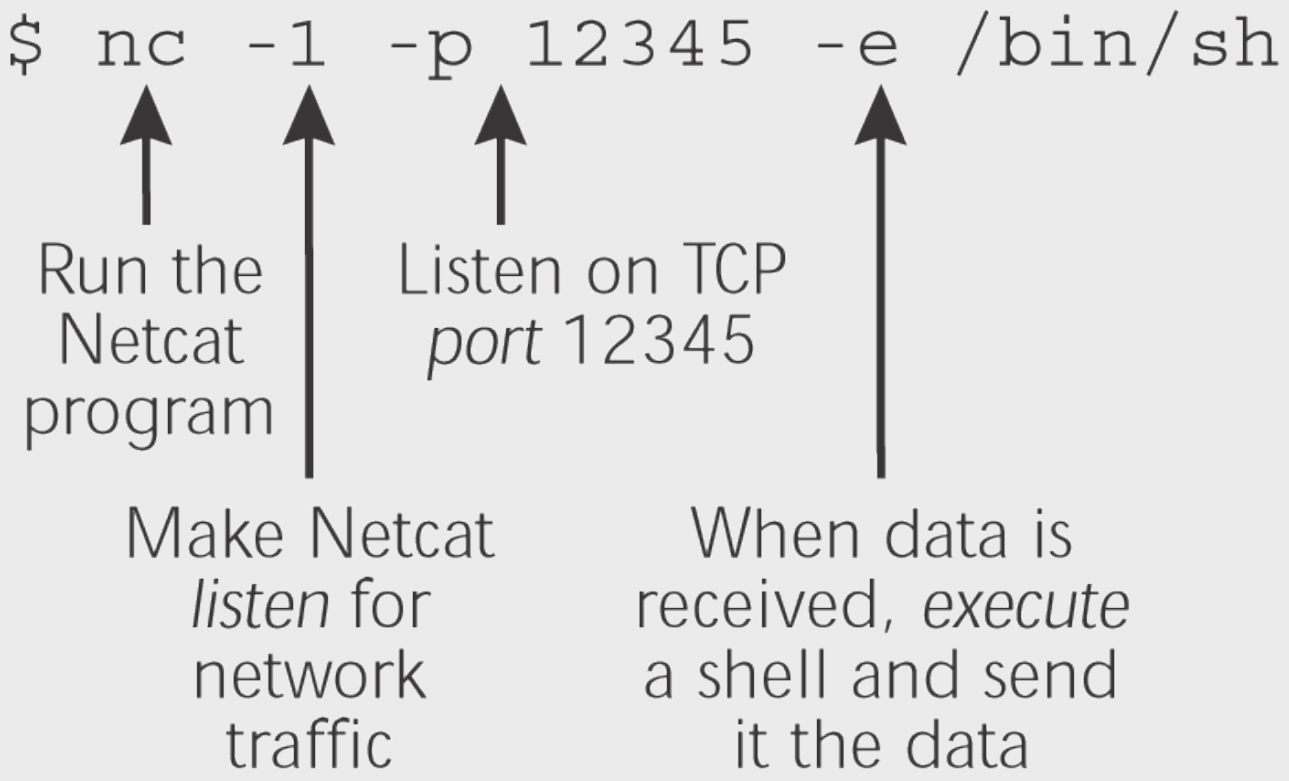
Backdoor

- Software that allows an attacker to access a machine using an alternative entry method
- Installed by attackers after a machine has been compromised
- May Permit attacker to access a computer without needing to provide account names and passwords
- Used in movie “War Games”
- Can be sshd listening to a port other than 22
- Can be setup using Netcat

Netcat as a Backdoor

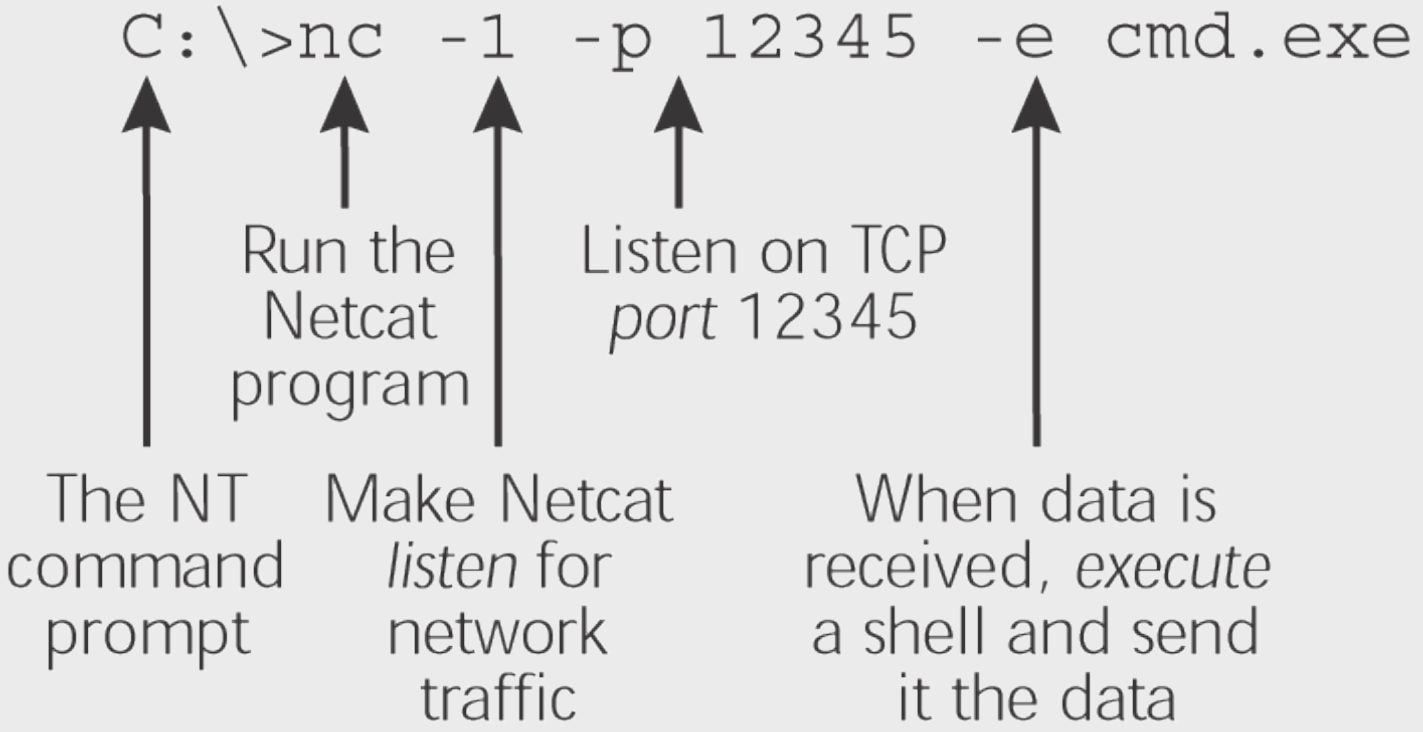
- A popular backdoor tool
- Netcat must be compiled with "GAPING_SECURITY_HOLE" option
- On victim machine, run Netcat in listener mode with –e flag to execute a specific program such as a command shell
- On attacker's machine run Netcat in client mode to connect to backdoor on victim

Running Netcat as a Backdoor on Unix



Note: on attacker's machine, run "nc victim 12345"

Running Netcat as a Backdoor on WinNT/2000



Trojan Horse Backdoors

- Programs that combine features of backdoors and Trojan horses
  - Not all backdoors are Trojan horses
  - Not all Trojan horses are backdoors
- Programs that seem useful but allows an attacker to access a system and bypass security controls

Categories of Trojan Horse Backdoors

- Application-level Trojan Horse Backdoor
  - A separate application runs on the system that provides backdoor access to attacker
- Traditional RootKits
  - Critical operating system executables are replaced by attacker to create backdoors and facilitate hiding
- Kernel-level RootKits
  - Operating system kernel itself is modified to allow backdoor access and to help attacker to hide

Application-level Trojan Horse Backdoor

- User must be tricked into installing this application which gives attacker backdoor access and complete control over victim's machine
- List of Application-level Trojan horse backdoor tools and default ports used http://www.simovits.com/nyheter9902.html
- Sub7 http://subseven.slak.org
- Back Orifice 2000 http://www.bo2k.com
- Hack-a-tack http://www.crokket.ce/hatboard/cgi-bin/pinboard.pl
- VNC www.uk.research.att.com/vnc

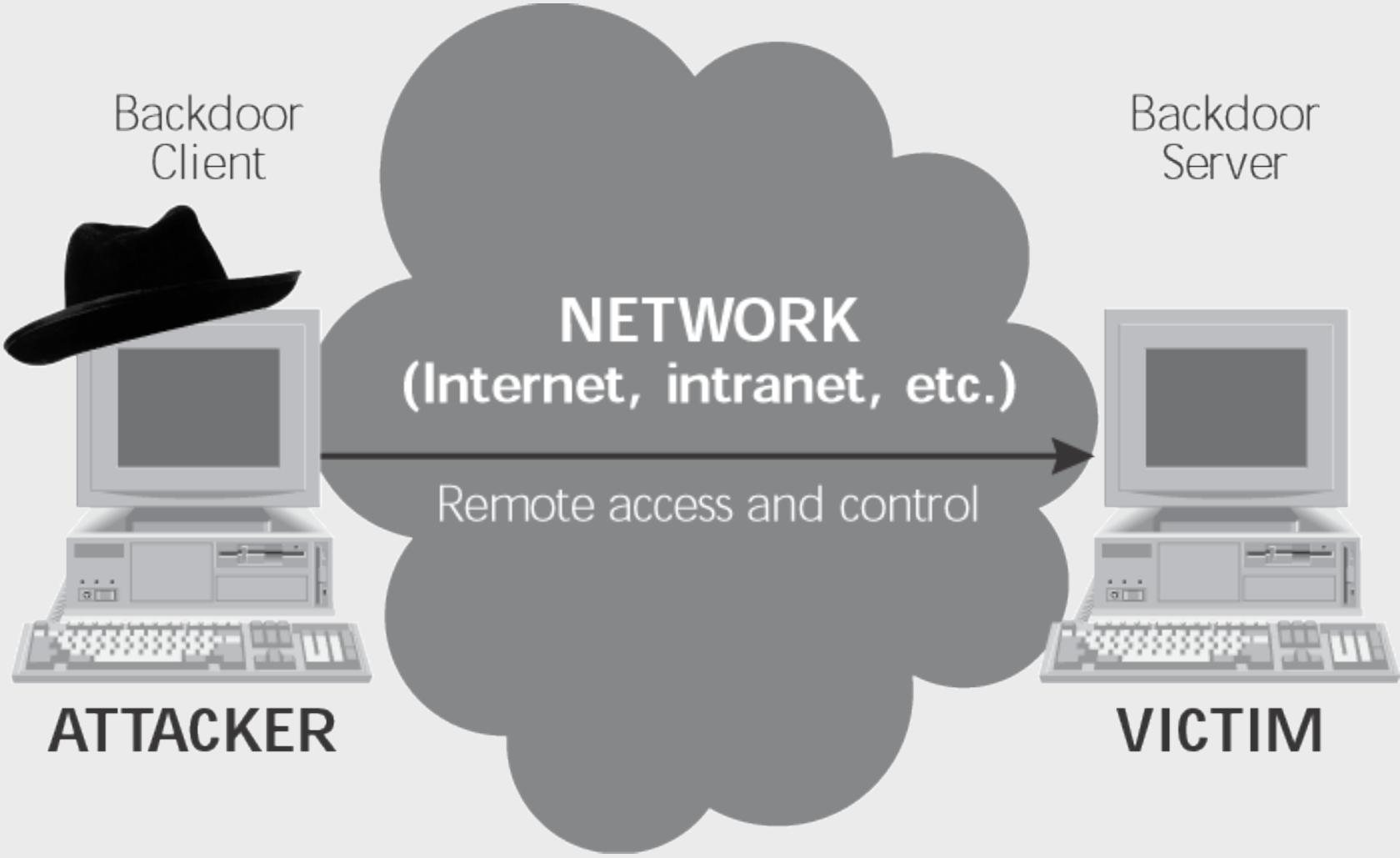


Figure 10.1 Attacker controls the Application-level Trojan horse backdoor on the victim across the network

Back Orifice 2000 (BO2K)

- Trojan horse backdoor http://www.bo2k.com
- May be legitimately used for system administration
- Product of Cult of the Dead Cow hacker group
- Released at DefCon 7 conference in 1999
- Video at http://www.uberspace.com
- Can undermine Windows 9x/ME and Windows NT/2000
- BO2K server code 100Kb
  - Can listen to any TCP or UDP port
  - Original Back Orifice listens to UDP port 31337
- BO2K GUI client code 500Kb

BO2K Capabilities

- Create popup dialog boxes
- Log keystrokes
- List detailed system information
- Gather passwords and dump SAM database
- View, copy, rename, delete, search, or compress any file on the system
- Edit, add, or remove any system or program configuration by changing the registry
- List, kill, or start any process
- Packet redirection to any other machine and port (relay)
- DOS-based application redirection (allows creation of Netcat backdoor)
- Multimedia control (allows attacker to view victim's screen and control keyboard)
- HTTP file server (for viewing victim's files via web browser)

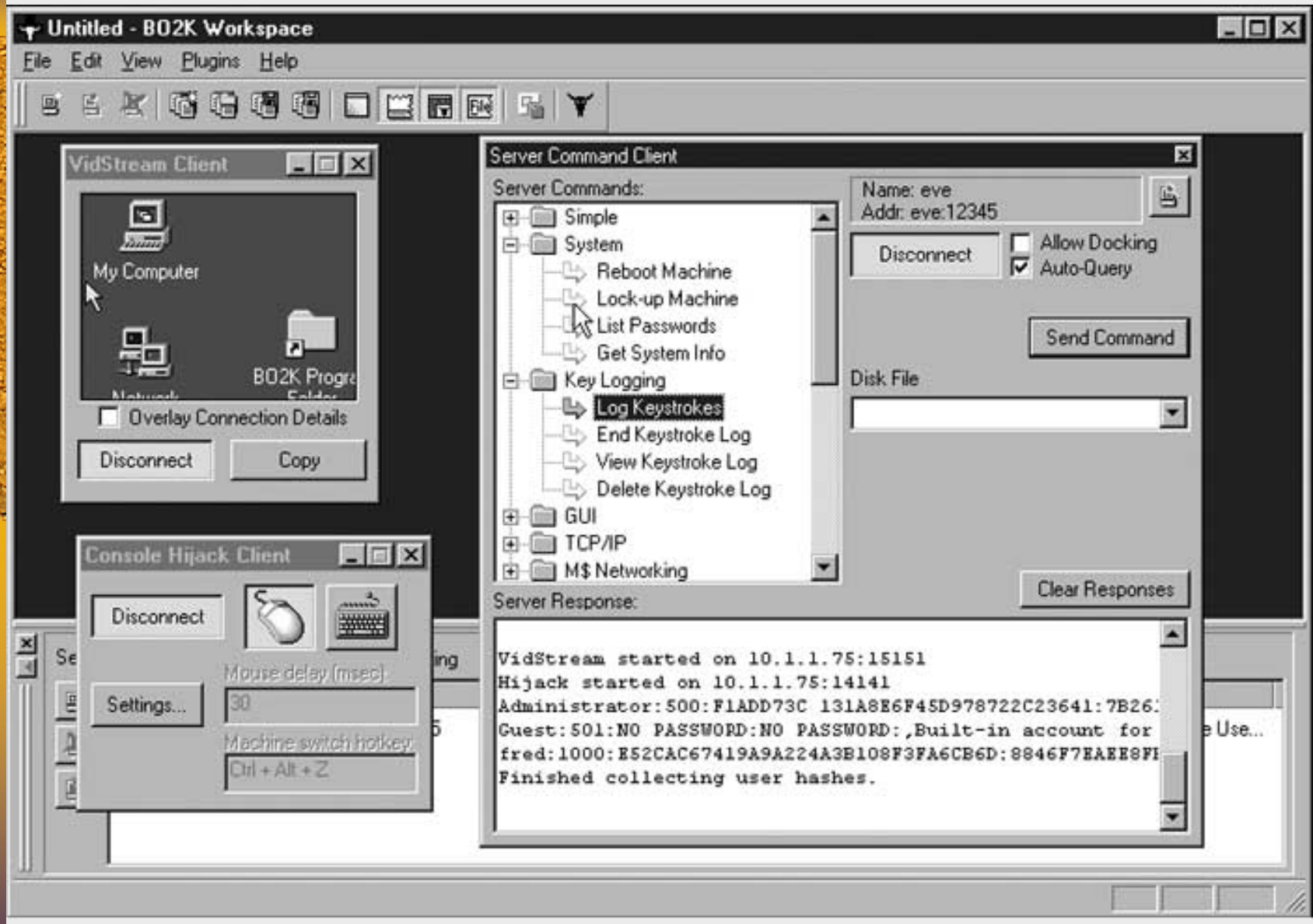


Figure 10.2 BO2K in use

Tricking Users to install Trojan Backdoors

- embed backdoor application in another innocent looking program via “wrappers”
- Wrapper creates one Trojan EXE application from two separate EXE programs
  - When Trojan EXE is run, both underlying EXE programs will run
  - Eg. Embed BO2K inside an electronic greeting card
  - Eg. Embed BO2K inside ActiveX programs on web servers
- Wrappers
  - Silk Rope http://www.netninja.com/bo/index.html
  - SaranWrap
  - EliteWrap

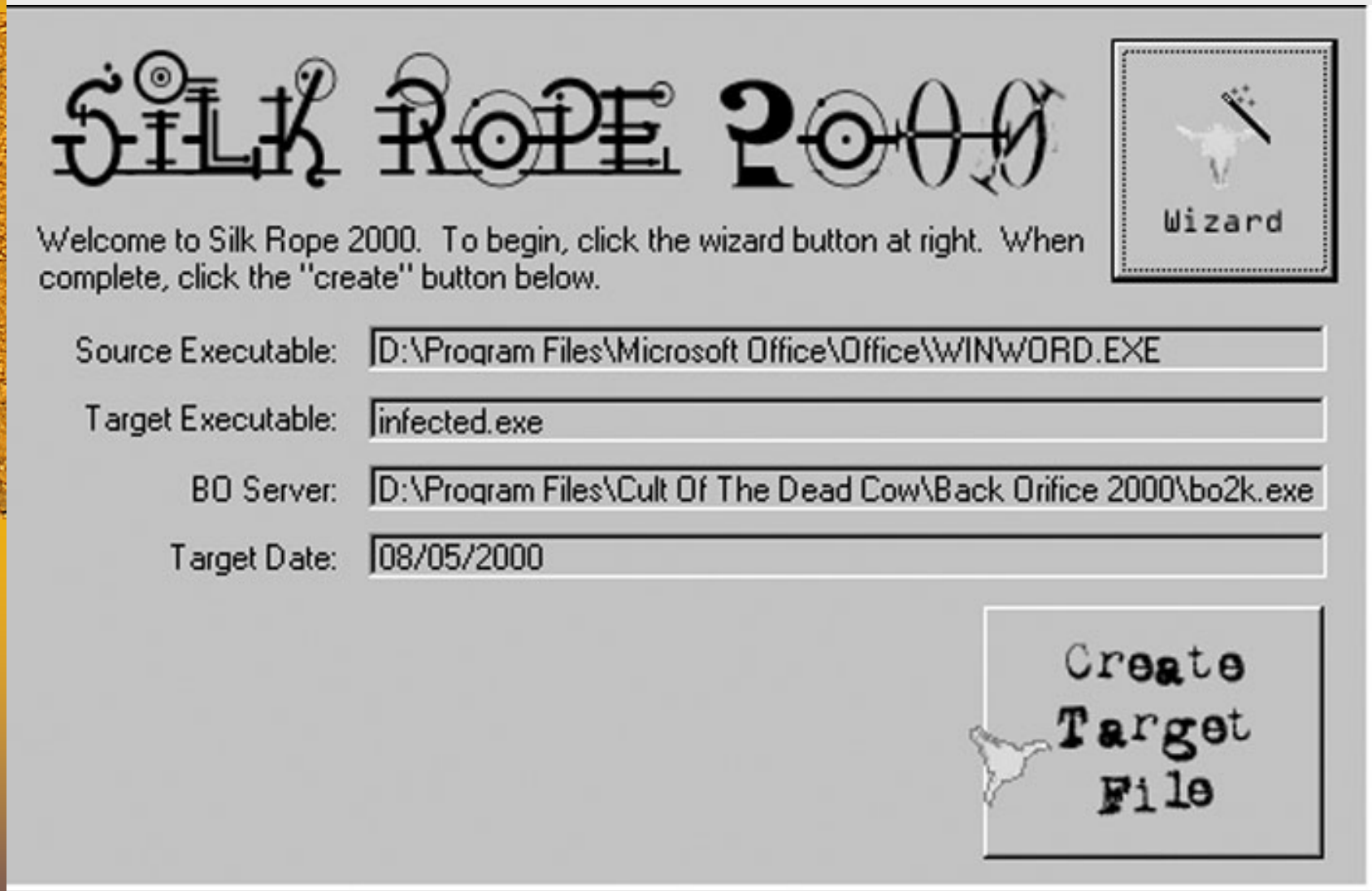


Figure 10.3 Make your own Trojan horse applications with Silk Rope

BO2K Plug-Ins

- Used to extend functionality of BO2K
- http://www.bo2k.com/warez.html
- BOPeep
  - Provides streaming video of victim's screen to attacker and allows attacker to hijack victim's keyboard and mouse
- Serpent, Blowfish, Cast256, IDEA, RC6 Encryption
  - Encrypts data between BO2K GUI and server

BO2K Plug-Ins (cont.)

- BOSOCK32
  - Provides stealth capabilities by using ICMP for transport instead of TCP or UDP
- Rattler, BT2K
  - Notifies attacker via email regarding location of BO2K servers
- Sniffer
  - Allows attacker to capture network traffic on victim ‘s LAN

Defenses against Application-Level Trojan Horse Backdoors

- Use antivirus tools
  - Can detect fingerprints (by checking filenames, registry key settings, services) of attack tools
  - Update virus definition files weekly
- Don’t use single-purpose BO2K checkers
  - Application itself may be a Trojan horse which installs BO2K but tells user that machine is clean

Defenses against Application-Level Trojan Horse Backdoors (cont.)

- Know your software
  - Only run software from trusted developers
  - Software should include a digital fingerprint to allow checking for trojanized program
  - http://www.rpmfind.net contains MD5 fingerprints of applications that can be checked via md5sum on Linux
  - Programs may be digitally signed by developer
- Educate your users
  - Web browsers should be configured not to run unsigned ActiveX controls
  - Block ActiveX controls without proper, trusted digital signatures at firewalls
  - Block Java applets that are signed by untrusted sources

tcpdump-3.4-29.i386 RPM - Microsoft Internet Explorer

File Edit View Favorites Tools Help Links

Back Forward Stop Refresh Home Search Favorites History Mail Print Real.com

Address http://rpmfind.net/linux/RPM/redhat/7.0/i386///tcpdump-3.4-29.i386.html Go

- kernel
- ld-linux.so.2
- libc.so.6

Copyright

BSD

Signatures

MD5: 1ccf1f47a294faafa0fd2ce464e1f1bf

GPG

Changelog

```
* Fri Aug 11 2000 Bill Nottingham <notting@redhat.com>
  - fix condrestart
* Fri Aug 11 2000 Jeff Johnson <jbj@redhat.com>
  - correct arpsnmp man pages (#15442).
  - don't print harmless ENOPROTOOPT message (#13518).
```

Done Internet

Figure 10.4 MD5 hash of tcpdump helps ensure it hasn’t been trojanized

Figure 10.5 Internet Explorer's security settings

Traditional RootKits

- A suite of tools that allow an attacker to maintain root-level access via a backdoor and hiding evidence of a system compromise
- More powerful than application-level Trojan horse backdoors(eg. BO2K, Netcat) since the latter run as separate programs which are easily detectable
- a more insidious form of Trojan horse backdoor than application-level counterparts since existing critical system components are replaced to let attacker have backdoor access and hide

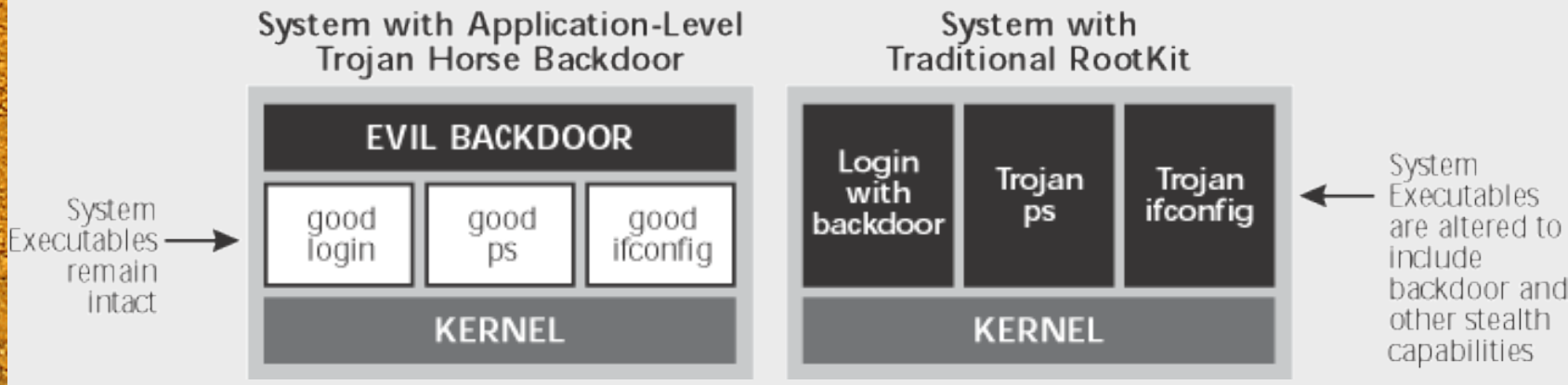


Figure 10.6 Comparing Application-level Trojan horse backdoors with traditional RootKits

Centerpiece of Traditional RootKits on Unix: /bin/login Replacement

- /bin/login program invoked to authenticate user whenever user logs in locally via keyboard or remotely (eg telnet)
- A RootKit replaces /bin/login with a modified version that includes a backdoor password for root access
  - Modified /bin/login is a backdoor since attacker still can get in even if the legitimate root password is changed
  - Modified /bin/login is a Trojan horse because is appears to be a normal login program
  - Facilitates hiding from “who” by not recording login into wtmp and utmp files if backdoor password is used

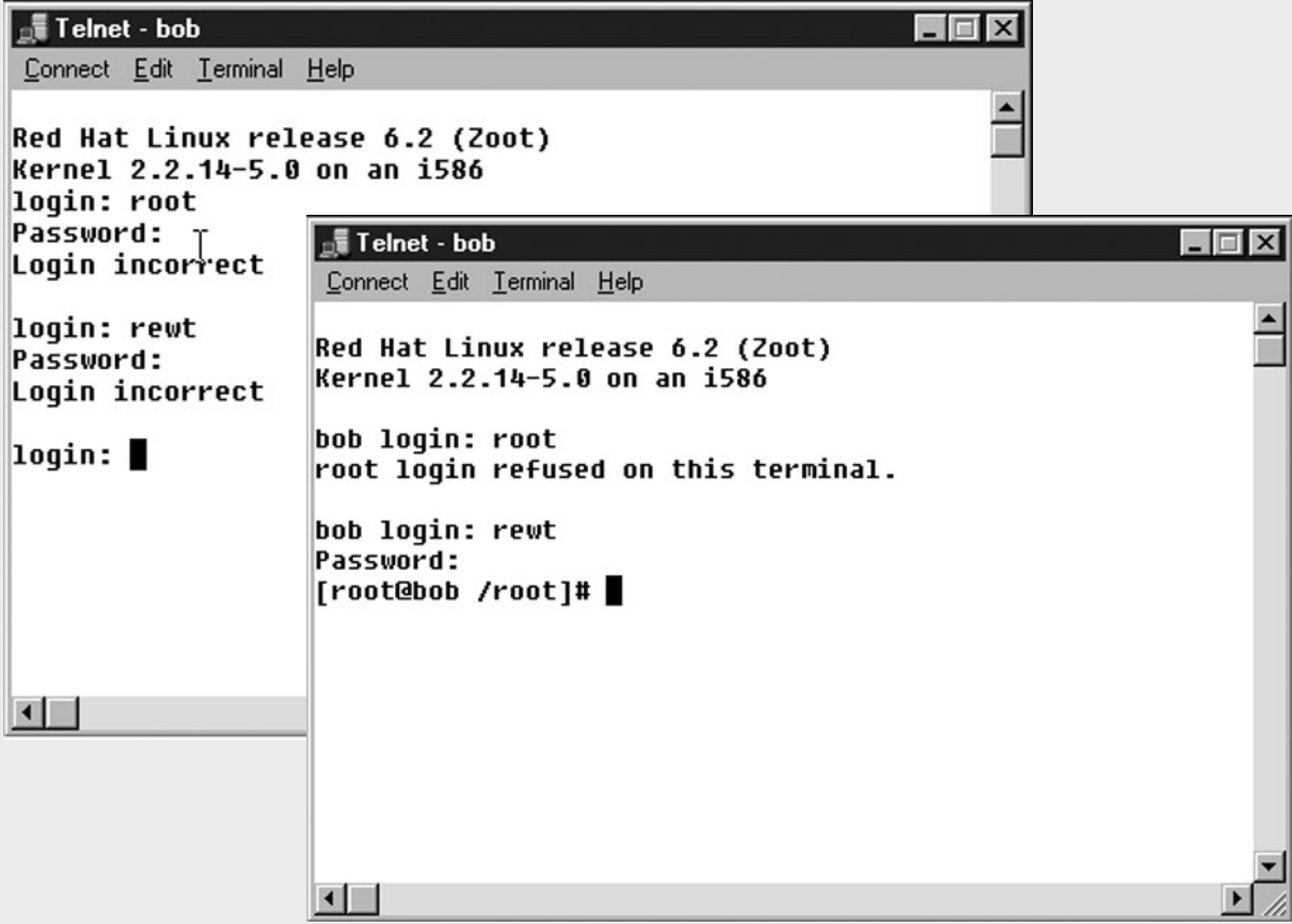


Figure 10.7 Behavior of /bin/login before (background) and after (foreground) installation of Linux RootKit “lrk5”

Detecting Traditional Rootkits

- Host-based IDS eg. Tripwire
- Strings command

Sniffing using Traditional RootKit

- Includes a sniffer that captures and writes into a file the first several characters of all sessions
  - Good for capturing userid/passwords in ftp, telnet, and login sessions
- Ifconfig on most Unix systems (except Solaris) will indicate whether NIC is in promiscuous mode
- Facilitates hiding of sniffer by including a trojanized ifconfig that lies about PROMISC flag

Telnet - bob

Connect Edit Terminal Help

```
[root@bob /root]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:10:4B:7B:EC:87
          inet addr:10.1.1.20  Bcast:10.1.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:3613 errors:0 dropped:0 overruns:0 frame:0
          TX packets:204 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:5 Base address:0x300

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:3924  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0

[root@bob /root]#
```

PROMISC flag is present, indicating that a sniffer is running.

Figure 10.8 ifconfig indicates sniffer use by showing PROMISC flag (except Solaris)

Programs typically replaced by RootKits

- du : Does not include disk space used by attacker
- find : Lies about presence of attacker’s files
- ifconfig : Masks promiscuous mode
- login : Contains backdoor root-level password for attacker
- ls : Lies about presence of attacker’s files
- netstat : Masks ports that are used by attacker
- ps : Lies about any process attacker wishes to hide
- inetd : modified to provide backdoor access
- syslogd : does not log attacker’s actions

Traditional RootKits in Use

- http://packetstorm/security.com/UNIX/penetration/rootkits
- Linux RootKit 5 (krk5)
  - Contains Trojan horse versions of chfn,chsh, crontab, du, find, ifconfig, inetd, killall, login, ls, netstat, passwd, pidof, ps, rshd, syslogd, tcpd, top, sshd, su
- T0rnkit for Linux and Solaris
  - Contains Trojan horse versions of login, ifconfig, ps, du, ls, netstat, in.fingerd, find, top

Defending against Traditional RootKits

- don’t let attacker get root in the first place
  - Use difficult to guess passwords
  - Apply patches
  - Close unused ports
- File integrity checkers
  - Create a read-only database of cryptographic hashes for critical system files, store these off line, and regularly compare hashes of the active programs to the stored hashes looking for changes
  - Tripwire http://ftp.cerias.purdue.edu/pub/tools/unix/ids/tripwire
  - Sun’s Solaris Fingerprint Database containing hases of critical Solaris executables http://sunsolve.Sun.com/pub-cgi/show.pl?target=content/content7

Recovering after being RootKitted

- Manually cleaning up after a RootKit installation is difficult
  - May miss finding all files that were changed
- Use most recent Tripwire-checked backup
- Reinstall all operating system components and applications

Kernel-Level RootKits

- More sinister, devious, and nasty than traditional RootKits
- Operating system kernel replaced by a Trojan horse kernel that appears to be well-behaved but in actuality is rotten to the core
- Critical system files such as ls, ps, du, ifconfig left unmodified
- Trojanized kernel can intercept system calls and run another application chosen by atttacker
  - Execution request to run /bin/login is mapped to /bin/backdoorlogin
  - Tripwire only checks unaltered system files
- If the kernel cannot be trusted, nothing on the system can be trusted

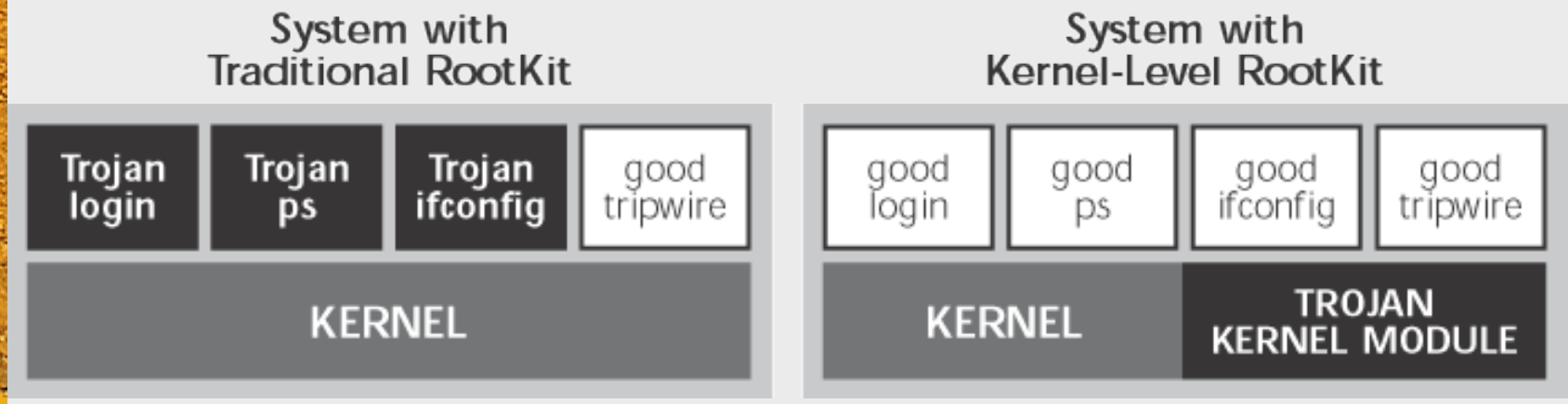


Figure 10.9 Comparing traditional RootKits with kernel-level RootKits

Kernel-Level RootKits (cont.)

- File Hiding
  - Attacker can hide specific subdirectories and files
- Process Hiding
  - Attacker can be running Netcat listener but the kernel will not report its existence to ps
- Network Hiding
  - Attacker can tell kernel to lie to netstat about network port being used by a backdoor program

Implementing Kernel-Level Rootkits

- Easiest way to modify kernel is to use the Loadable Kernel Module capability of operating system to extend the kernel
- To install the Knark RootKit on Linux, type “insmod knark.o” ; no reboot required
- Adore LKM RootKit for Linux
- Plasmoid LKM RootKit for Solaris
  - http://www.infowar.co.uk/thc/slkm-1.0html
- Kernel-level RootKit for WindowsNT
  - http://www.rootkit.com
  - A kernel patch not a LKM

Defending against Kernel-Level RootKits

- Don’t let attacker gain root in the first place
- Apply all relevant security patches
- Disable all unneeded services and ports
- Harden operating system
- Look for traces of kernel-level RootKits
  - Eg. Activate sniffer and check for presence of PROMISC flag in ifconfig
- Install chkrootkit ftp.pangeia.com/pub/seg/pac
- Install host-based IDS
- Build Linux kernels that don’t accept LKM