On The Edge: Protecting a Network Using Linux

Donald Thomas

Senior Member Technical Staff
HP

HP WORLD 2003
Solutions and Technology Conference & Expo

Agenda

- Introduction
- Attack
- Background
- Setup
- Firewall

Purpose

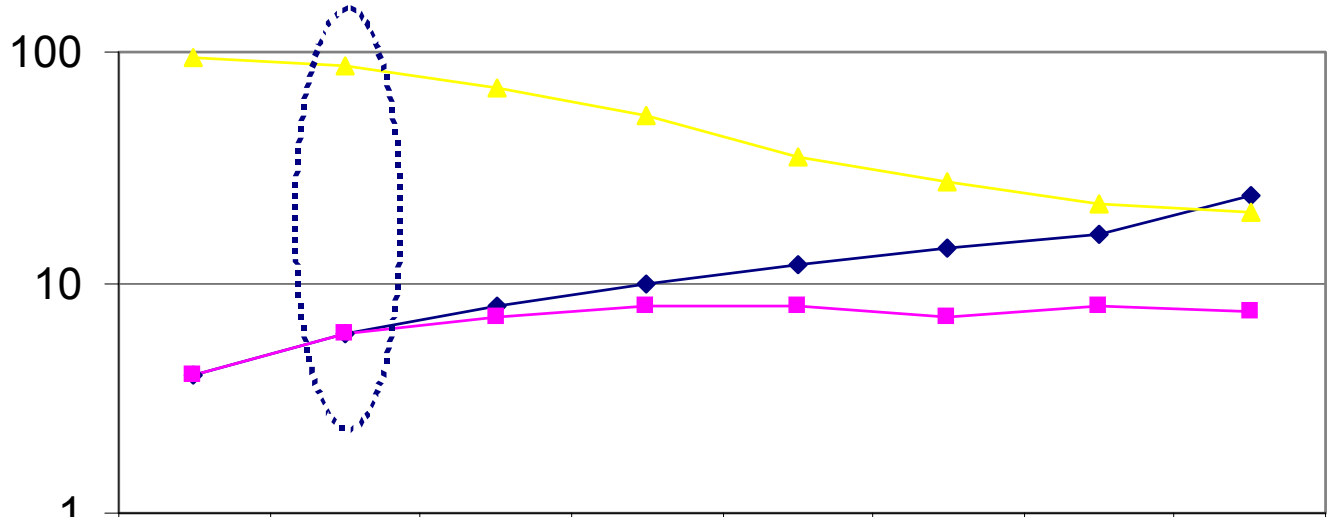
- Network protection from basic OS components
- Common sense approach
- Remove any mysteries around firewalling

Factoids

- Started with RHT 7.0 in July 2001
- Upgrades: 7.0 >> 7.2 >> 7.3 >> 8.0
- Only 2 intrusions since September 2001
  - Occurred within the first three months of operation
- DL380 G1

Goodies - 8way Performance

DL760 – 8 CPUs, 16MB memory, RHT AS2.1 (2.4.9-e.3)



	1	2	3	4	5	6	7	8
# of Threads	4	6	8	10	12	14	16	24
# of CPUs	4	6	7	8	8	7	8	8
CPU Load	95	86	70	53	35	27	22	20

Meatgrinder CPU Test Results
http://etd.cca.cpqcorp.net

Goodies - Storage

- Qlogic HBA and XP disk array
  - “sd” devices created during normal system boot. No special software needed.

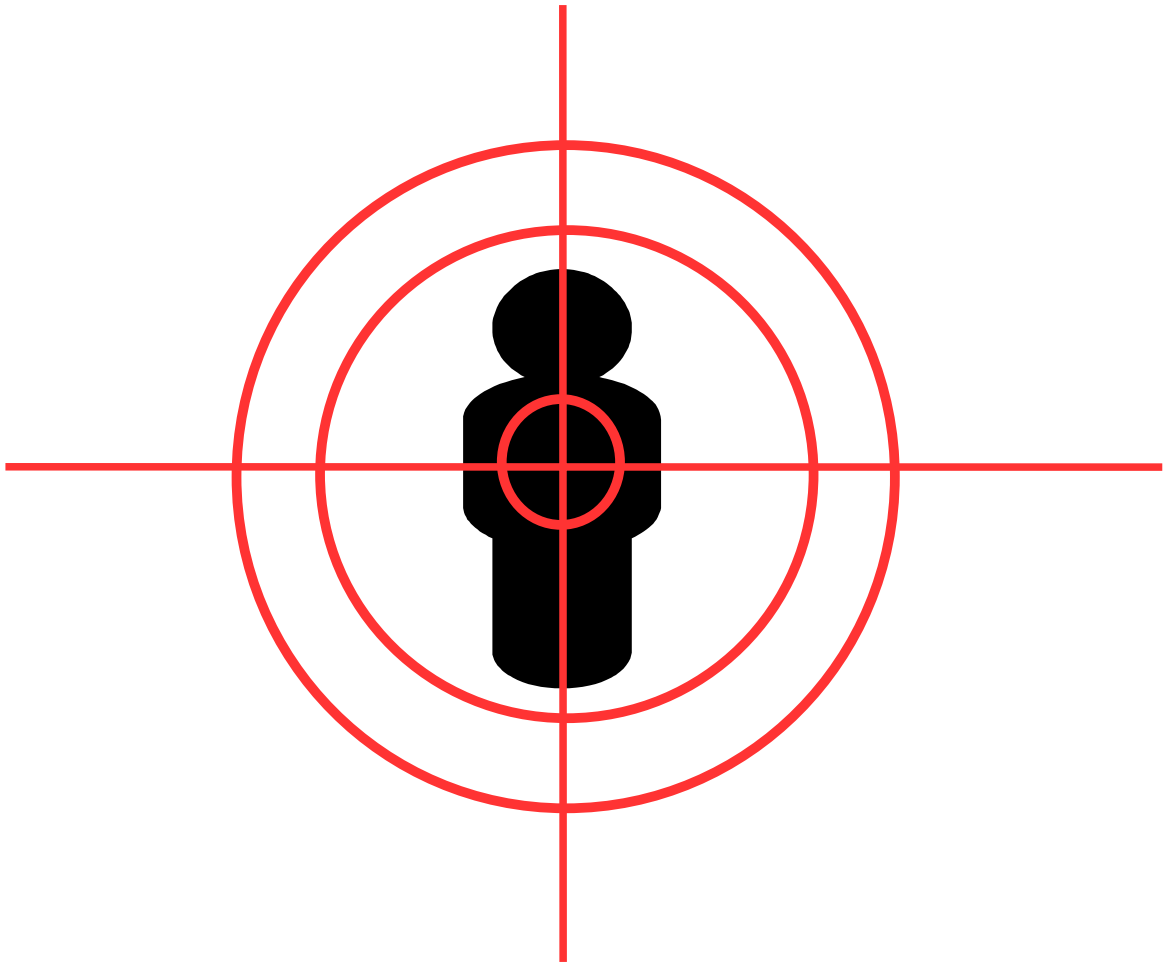
- Qlogic HBA and StorageWorks EVA
  - Requires installation of Linux Solution kit before devices (sda,sdb,sdc,etc.) can be accessed by the system.

Two Rules

1. Assume every packet has the potential to inflict damage.

2. Practice patience and be vigilant.

ATTACK!



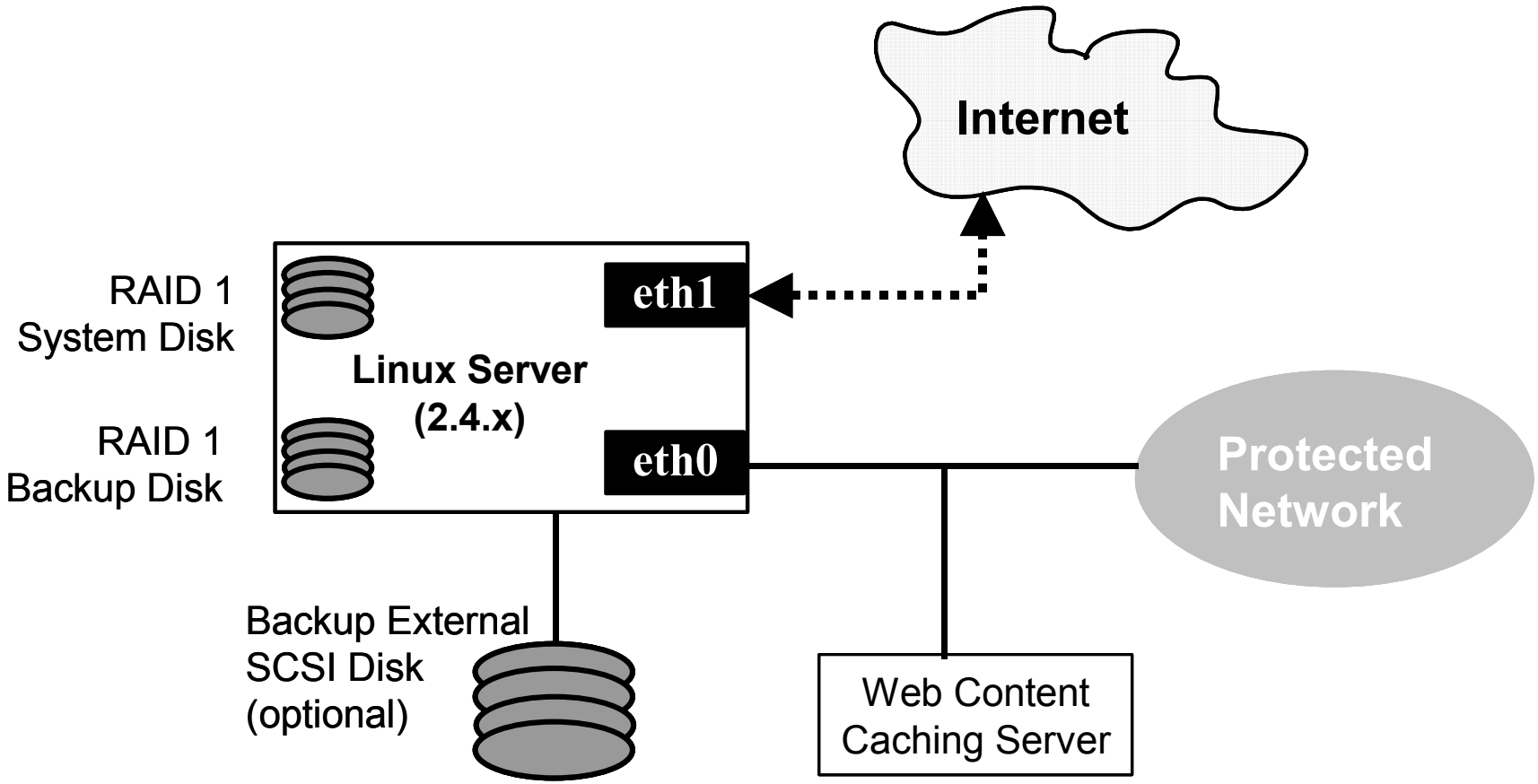
The Adversaries

- Hackers
  - Person or group who enjoy the challenge of breaking in
- Attackers
  - Person or group who intend to inflict damage to an environment
- Spies
  - Person or group who's primary intent is to illegally collect data from a network

Adversaries Cont'd

- Exploit Weaknesses
  - Protocols
  - Developer back doors
  - OS bugs
  - Command buffer overflows
- Hiding in the Shadows
  - Complex addressing schemes to avoid detection
- Modify System Programs
  - Affected programs work against you

A Basic Architecture



Preparation is Essential

- System Backup
  - Create a copy system disk
  - Use “dd” command

    dd if=/dev/cciss/c0d0 of=/dev/cciss/c0d1 bs=1024
  - Re-label copied disk to avoid same name disk labels if second disk will be online when system is bootedd.
- Monitoring
  - nmap - Tripwire
  - ethereal - tcpdump
  - netstat

Disk Backup

Disk Backup cont'd

2 – disk units

Disk Backup cont'd

/dev/cciss/**c0d0** → /dev/cciss/**c0d1**

"dd" copy time: 25 mins. for a 36.4GB disk

Disk Backup cont'd

Be careful not to switch disk positions!

SCSI ID in disk metadata does not change when disk positions change.

Disk Cloning

/dev/cciss/**c0d1** → /dev/cciss/**c0d0**

SCSI ID in disk metadata matches slot ID.

Preparation is Essential

- Logging
  - Re-direct logs away from host
  - /etc/syslog.conf

```
*.*    @remoteLoggingHostName
```

  - Check syslog service (514/udp)

Case Studies

Case #1 – "Leaf"

- Internet relay chat (ircd, #6667) used to gain access
- Remote ports: 5588 & 6667
- Local ports: 1025 & 1026
- The crontab facility was used to launch "leaf" program
- A directory, /dev/ptyas, with 777 perms was created by intruder to contain illegal programs
- The crontab program permissions were changed from '4755' to '0750'

Case #1 – "Leaf" cont'd

- /bin/login replaced with a "login" program from intruder
- /bin/login file attributes changed due to the file being replaced by the spy:
  - 1. Stripped vs. Non-stripped (command: file *)
  - 2. Install date of file changed to current date
- Spy IP addresses
  - 202.9.97.2
  - 95.121.6.196

Case #2 – "arkd00r"

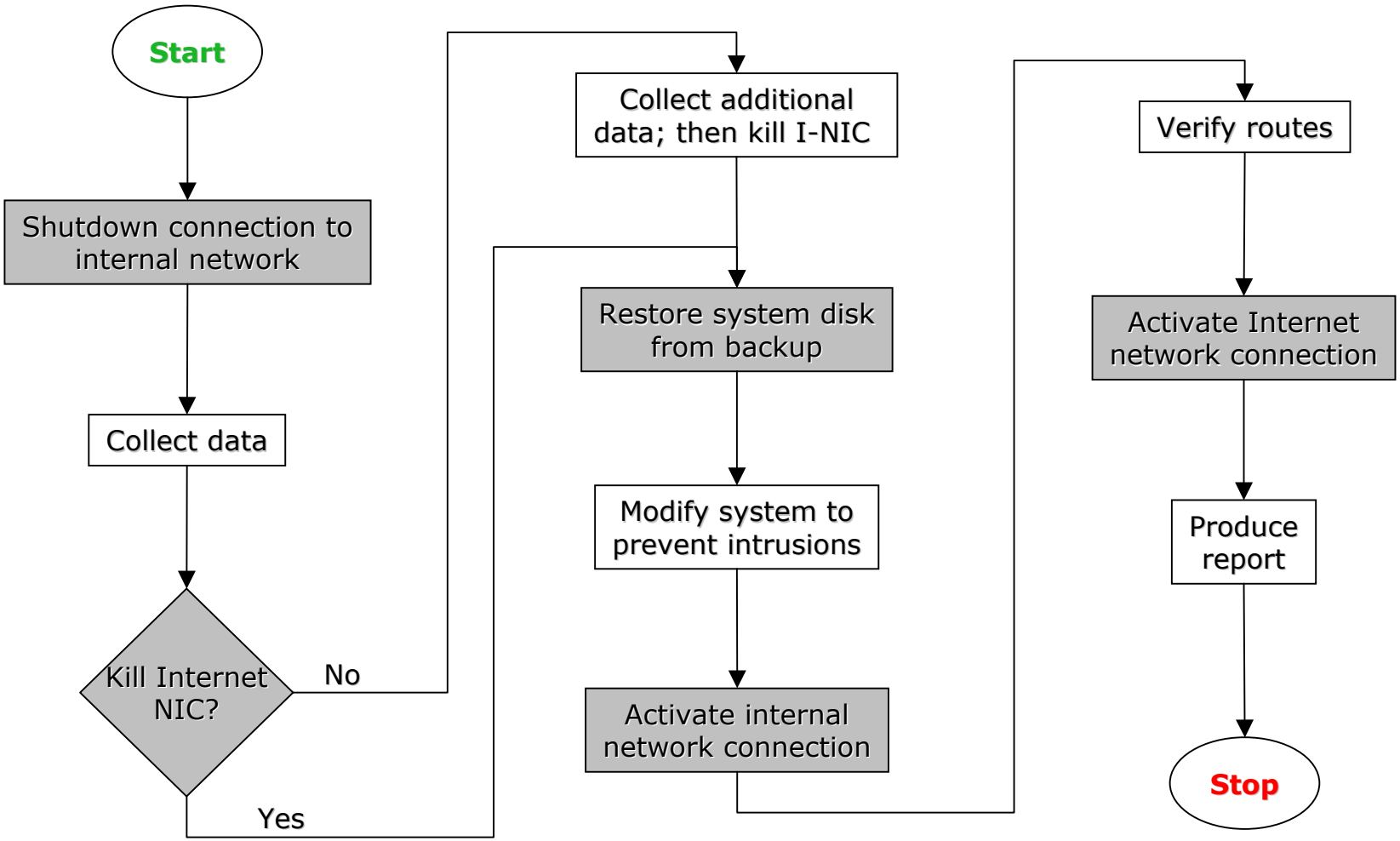
- Backdoor login ID named "arkd00r"
- ID provided access to a root shell
- Downloaded binaries: ps and login
- Setup processes that rotated TCP connections
- External TCP connections allowed spy to watch activity on server in realtime
- Killing "spy" processes degraded system performance
- Login to server only from system console

What to Do??

Objectives

- Remain calm
- Protect the internal network
- Preservation and collection of data on intruder

Post Intrusion Process



Post Intrusion Process cont'd

HP WORLD 2003
Solutions and Technology Conference & Expo

Incident Report Topics

- Impact to systems and network
- Sequence of events
- Actions taken
- Other contributing factors
- Next steps

Hardening the System

Hardening The System

- Installation
  - Use text mode, its faster
  - Select no firewall
  - Do not install everything
- Package Options

Printer support

Dialup workstation

Network management workstation

Utilities

Emacs

Development

Kernel development

Legacy Application support

Hardening The System cont'd

- Post-installation
  - Update NIC driver from HP web site
    - "Approved and tested"
      bcm5700, e100, e1000
  - Update cpqarray or cciss
    - "Approved and tested"
      /dev/ida , /dev/cciss
  - Check all routes to internal networks
  - Verify internal and external DNS access
- DO NOT CONNECT to outside world at this time
- Do a system backup (no firewall rules)

Hardening The System cont'd

File Permissions (chown)

- -R 751 /var/log
- 640 /var/log/messages
- 600 /etc/crontab
- 660 /var/log/wtmp
- 640 /var/log/lastlog
- 600 /etc/ftpusers
- 640 /etc/passwd
- 600 /etc/shadow
- -R 750 /etc/pam.d
- 600 /boot/grub/grub.conf
- 600 /etc/hosts.allow
- 600 /etc/hosts.deny
- 600 /etc/securetty
- 400 /etc/shutdown.allow
- 700 /etc/security
- -R 750 /etc/rc.d/init.d
- -R 751 /etc/sysconfig
- 400 /etc/cron.allow
- 400 /etc/cron.deny
- 400 /etc/sysctl.conf

Hardening The System cont'd

- /etc/services
  - www.iana.org/assignments/port-numbers
- /etc/resolv.conf
- /etc/sysctl.conf
- /etc/hosts
- /etc/sysconfig/network

Hardening The System cont'd

/etc/resolv.conf

```
search localdomain              #no domain
nameserver 10.17.0.254          #internal DNS
nameserver 199.101.83.207       #external DNS
```

/etc/sysctl.conf

```
net.ipv4.ip_forward = 0
net.ipv4.icmp_echo_ignore_all = 1
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

Hardening The System cont'd

/etc/hosts

```
127.0.0.1  localhost.localdomain localhost
192.168.0.1 privHostName        #eth0, internal net
161.104.222.44 pubHostName   #eth1, internet
```

/etc/sysconfig/network

```
HOSTNAME=pubHostName
FORWARD_IPV4=false
```

Firewalling

Firewalling

** IMPORTANT**

Before attempting to set IP forwarding and masquerading (NAT) on the server, all network IP addresses, gateway, and DNS addresses should be configured and working properly.

Firewalling cont'd

Minimum System Recommendations

- HP Proliant DL380 or DL360
- 2 – CPUs @ 900Mhz or better
- 2048 MB OF memory
- RAID 1 system disk
- RAID 0 or JBOD backup disk
- Partitions

  /boot = 256MB / = 6GB

  /home = 2GB swap = 1.5GB
- 2 - NICs

Firewalling cont'd

Main Script

```
# get common shell script functions
. /etc/init.d/functions
case "$1" in
'start')
    echo "1" > /proc/sys/net/ipv4/ip_forward
    action "Packet Forwarding enabled:" /etc/init.d/IPFstart.sh
;;

'stop')
     echo "0" > /proc/sys/net/ipv4/ip_forward
     action "Packet Forwarding disabled:" /etc/init.d/IPFstop.sh
;;
*)      echo "usage: $0 {start | stop}"
;;
esac
```

Firewalling cont'd

IPFstart.sh

- echo "1" > /proc/sys/net/ipv4/ip_forward
- iptables -t filter -A INPUT -s 10.32.0.0/12 -j ACCEPT
- iptables -t filter -A INPUT -i eth1 -p tcp --syn -j DROP
- iptables -t filter -A INPUT -i eth1 -p udp -j DROP
- iptables -P FORWARD ACCEPT
- iptables -t filter -A FORWARD -o eth1 -tcp -s 10.32.0.0/12 -j ACCEPT
- iptables -t nat -A POSTROUTING -s 10.32.0.0/12 -j SNAT --to-source 161.114.222.44

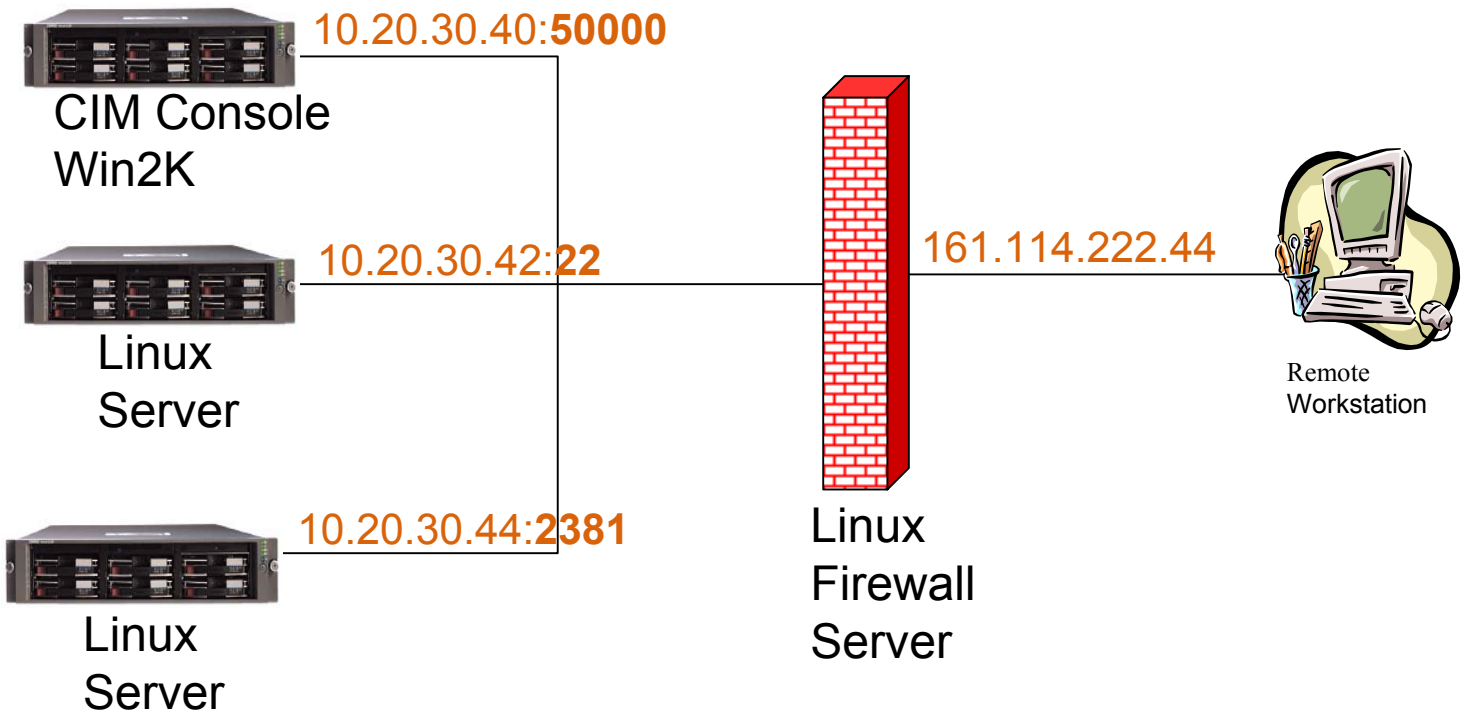
Firewalling cont'd

IPFstop.sh

```
echo "0" > /proc/sys/net/ipv4/ip_forward
iptables -t filter –F
iptables -t nat –F
iptables -t filter -P FORWARD DROP
```

Remote Access

Remote Access



Remote Access cont'd

- ssh

  iptables –t nat –A PREROUTING –i eth1 –p tcp –-dport 22 –j DNAT –-to-destination 10.20.30.42:22

- Inisght Manager 7

  iptables –t nat –A PREROUTING –i eth1 –p tcp –-dport 50000 –j DNAT –-to-destination 10.20.30.40:50000

- Management Agents

  iptables –t nat –A PREROUTING –i eth1 –p tcp –-dport 25000 –j DNAT –-to-destination 10.20.30.44:2381

Remote Access cont'd

- PPTP
  - http://pptpclient.sourceforge.net/howto-redhat-90.phtml
- PPTP show and tell
  - Linux on the laptop

Resources

- http://linux..cca.cpqcorp.net/
- http://www.hp.com/linux
- Me – Don Thomas

  dk.thomas@hp.com

  281-927-8460

Interex, Encompass and HP bring you a powerful new HP World.

Fonts, capitalization, emphasis and subdues

- Titles are Verdana bold 30 point
- Main bullet items are Arial 26 point
  - Sub bullets Arial 24 point
- Initial cap first word all titles and text
- Emphasize **keywords** Arial bold… R217, G99, B11
- Subdued text (including the bullet)should be treated as such… R128, G128, B128

Color palette

Fill and accent colors

11 131 179	122 162 68	217 99 11	237 195 43

Additional colors

197 52 58	208 52 119	33 94 155	138 121 103

On ALL slides, DO NOT extend text beyond this safe area