

Fun with SOHO Router 101

by Jhe@HITCON-CMT

Who am I ?

- Jhe
- Co-founder of UCCU
- know a little
 - Web security
 - Binary exploitation
 - Parseltongue (python)

What is SOHO Router

Firmware overview

Reversing engineering

Common vulnerabilities

Real world case

UCCU

What is SOHO Router

Firmware overview

Reversing engineering

Common vulnerabilities

Real world case

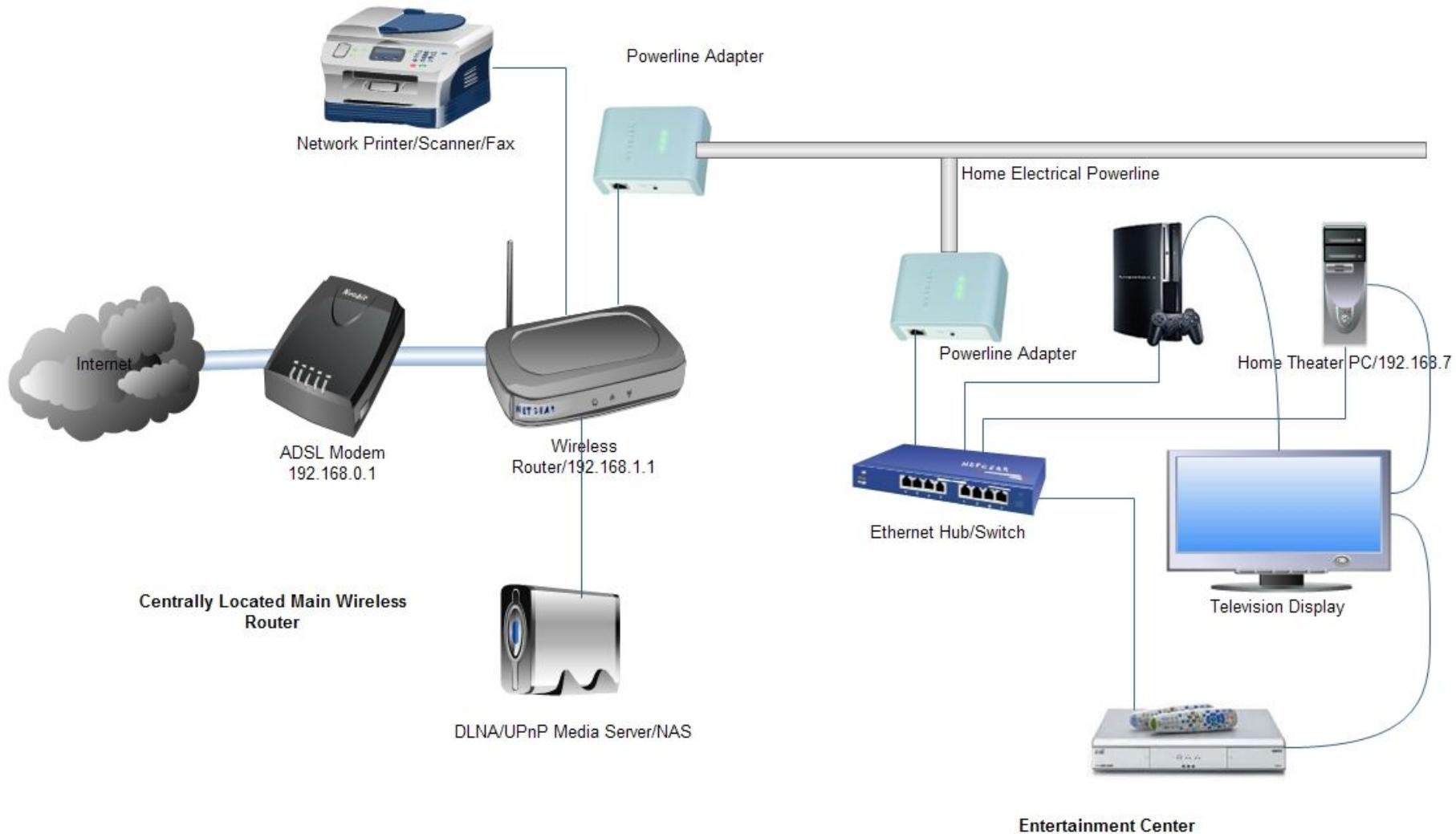
UCCU

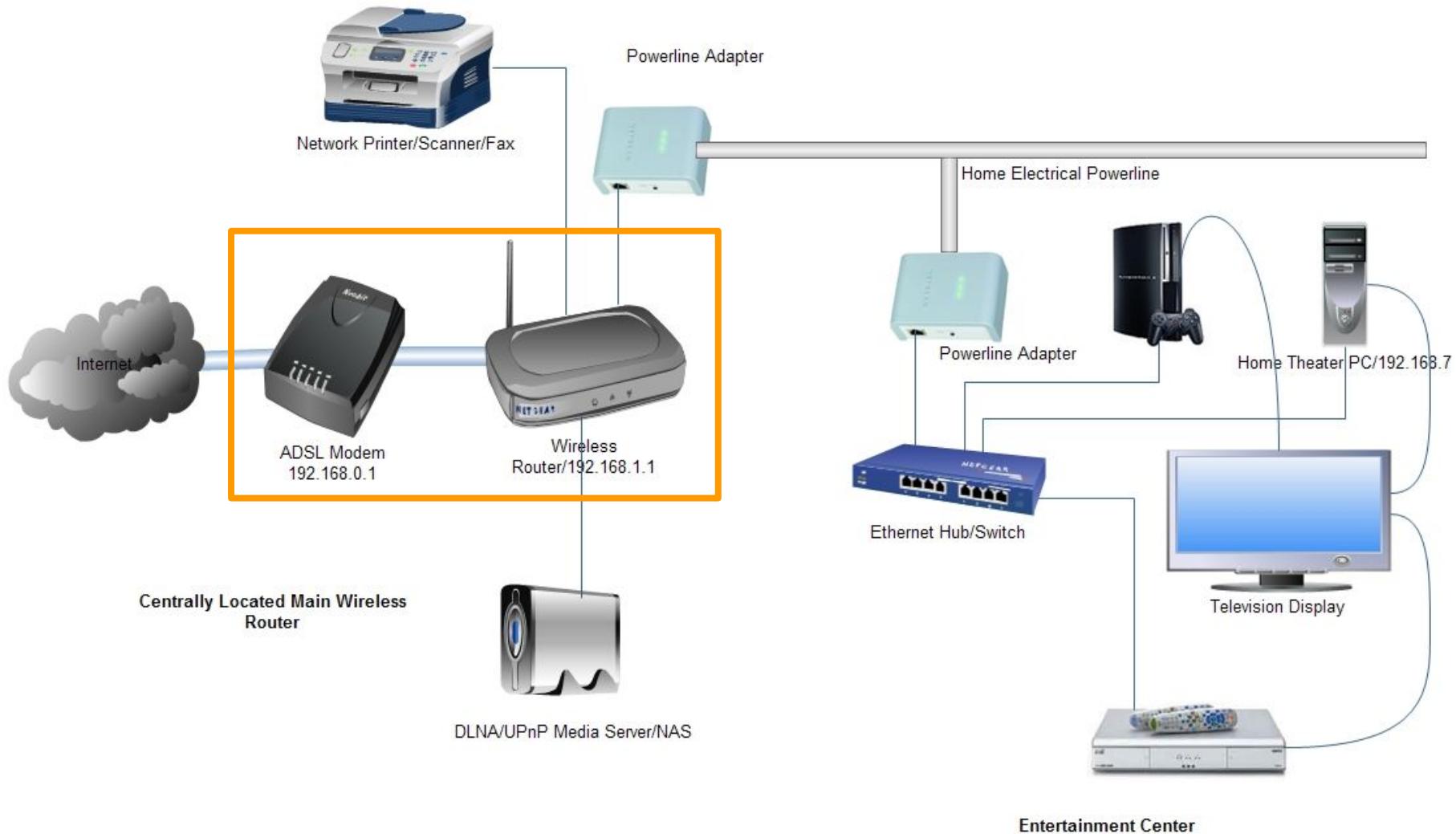
What is SOHO Router

- Small Office / Home Office
- functions
 - NAT, VPN, Dynamic DNS,
 - Port forwarding, Firewall, Wireless
 - DHCP, MAC filter, Remote Mgt.
 - Ad. block

What is SOHO Router

- Small Office / Home Office
 - functions
 - NAT, VPN, Dynamic DNS,
 - Port forwarding, Firewall, Wireless
 - DHCP, MAC filter, Remote Mgt.
 - Ad. block
- 







TP-LINK®
The Reliable Choice

D-Link®
Building Networks for People

LINKSYS™

Tenda®

net•core 磊科

NETGEAR®

What is SOHO Router

Firmware overview

Reversing engineering

Common vulnerabilities

Real world case

UCCU

Firmware overview

Two ways to debug

- Hardware
 - JTAG, Serial / UART console ...
- Software
 - Just download it from official website

Firmware overview

Two ways to debug

- Hardware
 - JTAG, Serial / UART console ...
- Software
 - Just download it from official website

Firmware overview

- File system
 - SquashFS, JFFS2, cramfs, YAFFS ...
- Architecture
 - MIPS/MIPSEL, ARM, PPC, x86, x86-64 ...
- Bootloader

What is SOHO Router

Firmware overview

Reversing engineering

Common vulnerabilities

Real world case

UCCU

Reversing engineering

- Static analysis
 - firmware extraction
 - reversing binary (IDA Pro ...)
 - something hardcoded
 - open source code
 - known vulnerabilities

Reversing engineering

- Dynamic analysis
 - **firmware extraction**
 - run with emulator(QEMU, Gdb, IDA Pro)
 - port scanning
 - Web security testing

Reversing engineering

Prerequisite

- binwalk
 - analysis, reverse engineering,
extracting

Reversing engineering

Prerequisite

- binwalk
- fmk (firmware mod kit)
 - build firmware, unsquash, uncramfs ...

Reversing engineering

Prerequisite

- binwalk
- fmk
- Linux

Reversing engineering

Extraction

```
[~/Security/Firmware/BR_6430nS/BR-6430nS_v1.15]> file BR-6430nS_v1.15.bin  
BR-6430nS_v1.15.bin: data  
[jne@arcn] [/dev/pts/1]  
[~/Security/Firmware/BR_6430nS/BR-6430nS_v1.15]> binwalk BR-6430nS_v1.15.bin
```

DECIMAL	HEXADECIMAL	DESCRIPTION

11280	0x2C10	LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 2301952 bytes
655360	0xA0000	Squashfs filesystem, big endian, version 2.0, size: 1285994 bytes, 500 inodes, blocksize: 65536 bytes, created: 2013-10-11 06:34:54

Reversing engineering

Extraction

```
[~/Security/Firmware/BR_6430nS/BR-6430nS_v1.15]> file BR-6430nS_v1.15.bin  
BR-6430nS_v1.15.bin: data  
[jhe@arch] [/dev/pts/1]  
[~/Security/Firmware/BR_6430nS/BR-6430nS_v1.15]> binwalk BR-6430nS_v1.15.bin
```

DECIMAL	HEXADECIMAL	DESCRIPTION

11280	0x2C10	LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 2301952 bytes
655360	0xA0000	Squashfs filesystem, big endian, version 2.0, size: 1285994 bytes, 500 inodes, blocksize: 65536 bytes, created: 2013-10-11 06:34:54

Reversing engineering

Extraction

```
[~/Security/Firmware/BR_6430nS/BR-6430nS_v1.15]> file BR-6430nS_v1.15.bin  
BR-6430nS_v1.15.bin: data  
[jhe@arch] [/dev/pts/1]  
[~/Security/Firmware/BR_6430nS/BR-6430nS_v1.15]> binwalk BR-6430nS_v1.15.bin
```

DECIMAL	HEXADECIMAL	DESCRIPTION

11280	0x2C10	LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size: 2301952 bytes
655360	0xA0000	Squashfs filesystem, big endian, version 2.0, size: 1285994 bytes, 500 inodes, blocksize: 65536 bytes, created: 2013-10-11 06:34:54

Reversing engineering

Extraction

```
[~/Security/Firmware/BR_6430nS/BR-6430nS_v1.15]> binwalk BR-6430nS_v1.15.bin
```

DECIMAL	HEXADECIMAL	DESCRIPTION
<hr/>		
11280 e: 2301952 bytes	0x2C10	LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size
655360 : 65536 bytes, created: 2013-10-11 06:34:54	0xA0000	Squashfs filesystem, big endian, version 2.0, size: 1285994 bytes, 500 inodes, blocksize

```
[~/Security/Firmware/BR_6430nS/BR-6430nS_v1.15]> dd if=BR-6430nS_v1.15.bin bs=1 skip=655360 of=squashfs.out  
1286146+0 records in  
1286146+0 records out  
1286146 bytes (1.3 MB, 1.2 MiB) copied, 2.71206 s, 474 kB/s
```

```
[jhe@arch] [/dev/pts/1]
```

```
[~/Security/Firmware/BR_6430nS/BR-6430nS_v1.15]> file squashfs.out
```

```
squashfs.out: Squashfs filesystem, big endian, version 2.0, 1285994 bytes, 500 inodes, blocksize: 65536 bytes, created  
: Fri Oct 11 06:34:54 2013
```

Reversing engineering

Extraction

```
[~/Security/Firmware/BR_6430nS/BR-6430nS_v1.15]> binwalk BR-6430nS_v1.15.bin
```

DECIMAL	HEXADECIMAL	DESCRIPTION

11280 e: 2301952 bytes	0x2C10	LZMA compressed data, properties: 0x5D, dictionary size: 8388608 bytes, uncompressed size
655360 : 65536 bytes, created: 2013-10-11 06:34:54	0xA0000	Squashfs filesystem, big endian, version 2.0, size: 1285994 bytes, 500 inodes, blocksize

```
[~/Security/Firmware/BR_6430nS/BR-6430nS_v1.15]> dd if=BR-6430nS_v1.15.bin bs=1 skip=655360 of=squashfs.out  
1286146+0 records in  
1286146+0 records out  
1286146 bytes (1.3 MB, 1.2 MiB) copied, 2.71206 s, 474 kB/s
```

```
[jhe@arch] [/dev/pts/1]
```

```
[~/Security/Firmware/BR_6430nS/BR-6430nS_v1.15]> file squashfs.out  
squashfs.out: Squashfs filesystem, big endian, version 2.0, 1285994 bytes, 500 inodes, blocksize: 65536 bytes, created  
: Fri Oct 11 06:34:54 2013
```

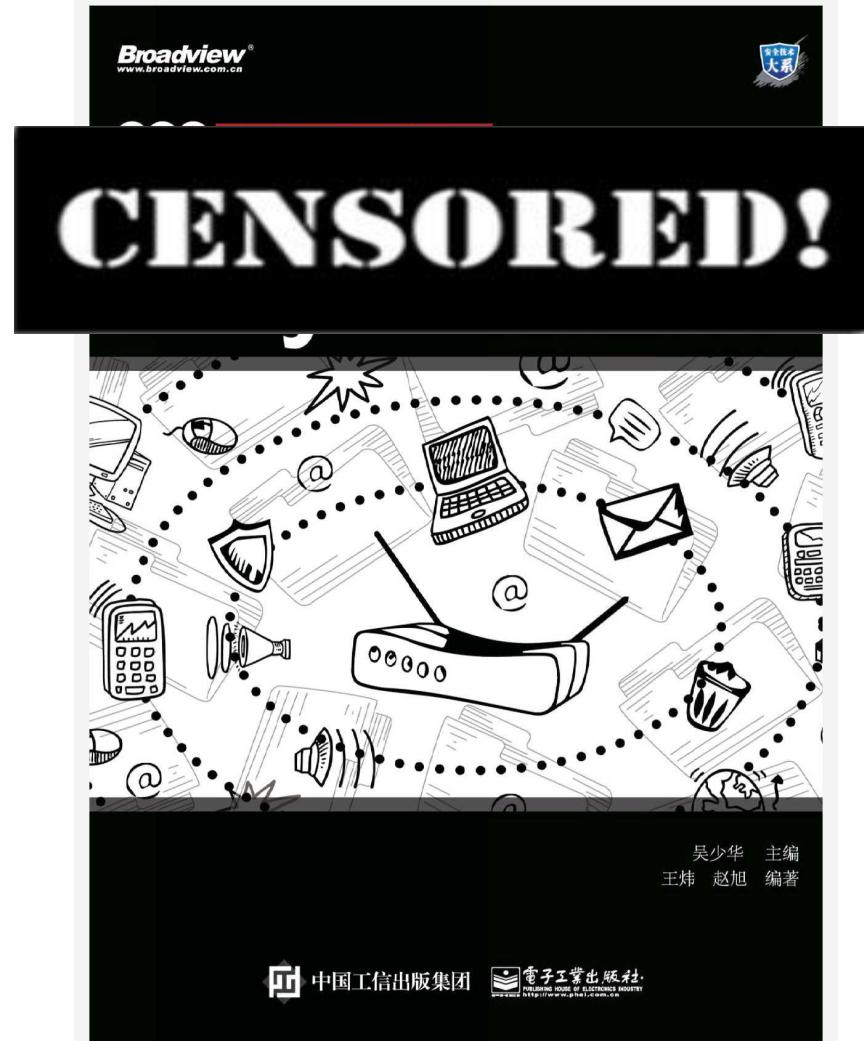
Reversing engineering

Extraction

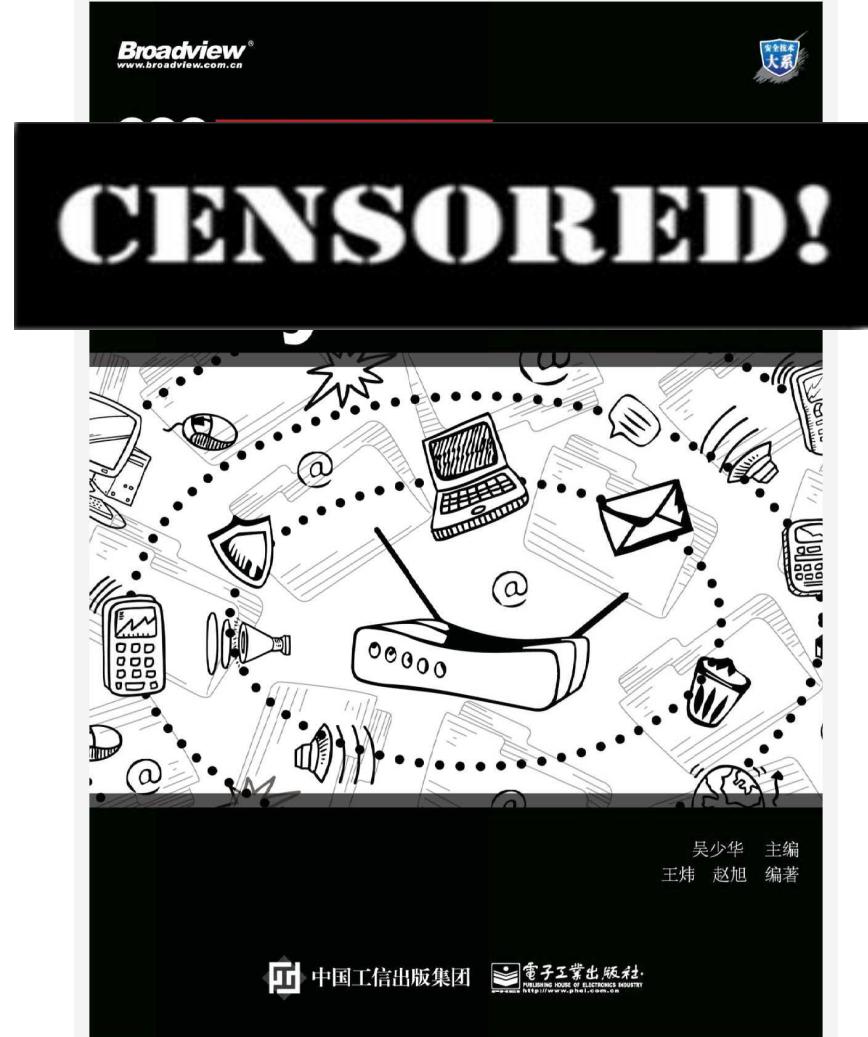
```
[~/Security/Firmware/BR_6430nS/BR-6430nS_v1.15]> ../../fmk/unsquashfs_all.sh squashfs.out
Attempting to extract SquashFS .X file system...

Trying ./src/squashfs-2.1-r2/unsquashfs-lzma...
created 370 files
created 34 directories
created 67 symlinks
created 0 devices
created 0 fifos
File system sucessfully extracted!
MKFS="./src/squashfs-2.1-r2/mksquashfs-lzma"
```

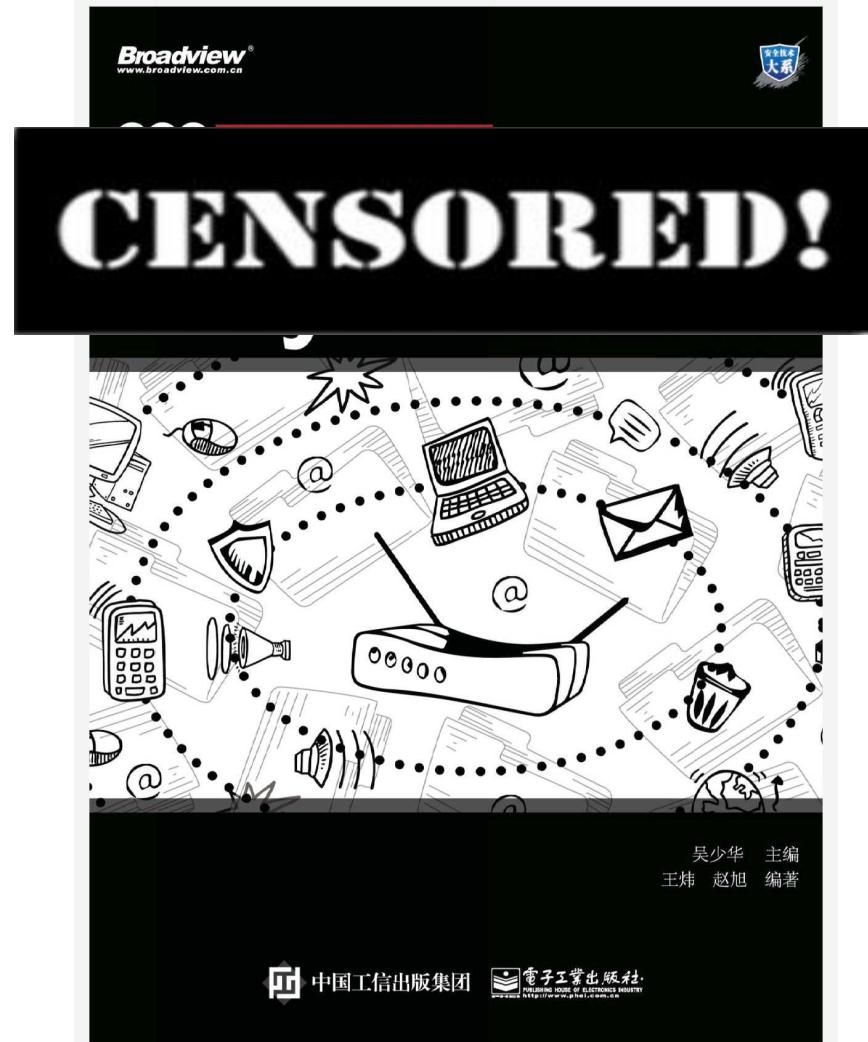
Some of you
may have
this



It is true



But not that
easy



Example

build emulation environment

- QEMU(arm, mips, mipsel)
- Cross-compilation

Example

repair runtime environment

1. run with QEMU
2. **if** ERROR_ECCURRED **then**
 - function hijacking with LD_PRELOAD
 - goto** 1

Firmadyne

- System for emulation and dynamic analysis of Linux-based firmware
- Toolchain
- Console
- Nvram
- Testing with metasploit framework

What is SOHO Router

Firmware overview

Reversing engineering

Common vulnerabilities

Real world case

UCCU

Common vulnerabilities

- XSS, CSRF
- Command Injection
- Denial of Service
- Information Disclosure
- Weak / Default Password

Common vulnerabilities

- Broken Authentication
- Buffer overflow
- Backdoor

Common vulnerabilities

- Broken Authentication
- Buffer overflow
- Backdoor



What is SOHO Router

Firmware overview

Reversing engineering

Common vulnerabilities

Real world case

UCCU

Real world case

BR_6430nS_v1.15

- why this one ?

Real world case

BR_6430nS_v1.15

- why this one ?
- short story

Real world case

BR_6430nS_v1.15

- why this one ?
- short story



http://CENSORED/w/Image/Firmware/Wireless/Router/BR-6430nC_nS/BR-6430nS_v1.17.zip

Real world case

BR_6430nS_v1.15

- why this one ?
- short story



CENSORED!

http://w/Image/Firmware/Wireless/Router/BR-6430nC_nS/BR-6430nS_v1.17.zip

Real world case

BR_6430nS_v1.15

- why this one ?
- short story

 [http://CENSORED!](#) w/Image/Firmware/Wireless/Router/BR-6430nC_nS/BR-6430nS_v1.17.zip

 [http://CENSORED!](#) w/Image/Firmware/Wireless/Router/BR-6430nC_nS/BR-6430nS_v1.15.zip

Real world case

Real world case

```
[~/Security/Firmware/BR_6430nS/BR-6430nS_v1.15]> ls  
BR-6430nS_v1.15.bin  squashfs.out  squashfs-root
```

Real world case

```
[~/Security/Firmware/BR_6430nS/BR-6430nS_v1.15]> ls  
BR-6430nS_v1.15.bin  squashfs.out  squashfs-root
```

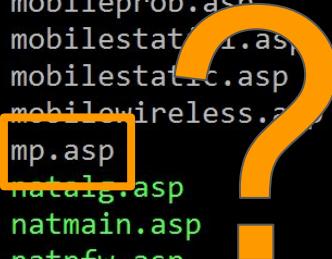
```
[~/Security/Firmware/BR_6430nS/BR-6430nS_v1.15/squashfs-root]> ls  
bin  dev  etc  lib  linuxrc  proc  sbin  tmp  usr  var  web
```

Real world case

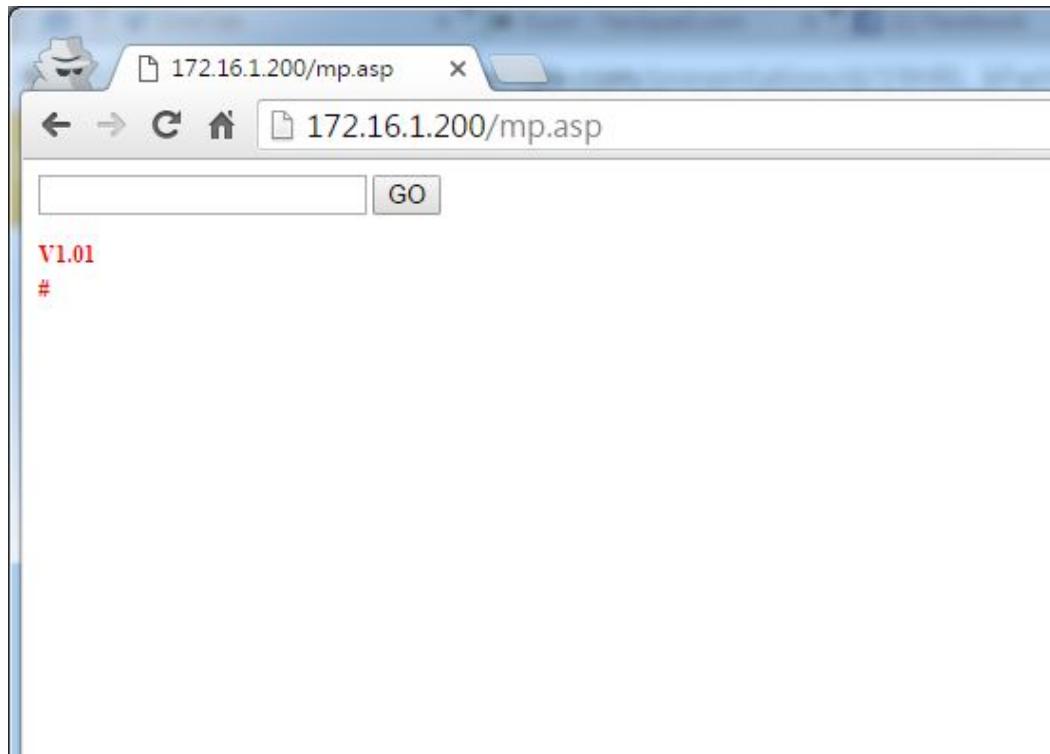
```
[~/Security/Firmware/BR_6430nS/BR-6430nS_v1.15/squashfs-root/web]> ls  
ezqos.asp          iQsetup_pppoe1.asp    mobilepppoe1.asp    stasylog.asp      wanwisp.asp  
file               iQsetup_pppoe.asp    mobilepppoe.asp    status.asp       wladvance.asp  
FUNCTION_SCRIPT    iQsetup_prob.asp    mobileprob.asp    style.css        wlbasic.asp  
fwcontrol.asp      iQsetup_static1.asp   mobilestatic1.asp syspasswd.asp    wlcontrol.asp  
fwdmz.asp          iQsetup_static.asp   mobilestatic.asp  sysrm.asp       wlencrypt.asp  
fwdos.asp          iQsetup_wireless.asp  mobilewireless.asp systimezone.asp wlschedule.asp  
fwmain.asp         javascript.js      mp.asp           tlcon.asp       wlstatbl.asp  
fwurlb.asp         lan.asp           natalg.asp       tlreset.asp     wlsurvey2.asp  
iQsetup.asp        language.asp      natmain.asp      tlreset_inner.htm wlsurvey.asp  
iQsetup_check.asp  mobilecheck.asp   natpfw.asp      tlupgrade.asp   wlwdsenp3.asp  
iQsetup_detect.asp mobiledetect.asp  natupnp.asp     tlupgrade_inner.asp wlwdsenp4.asp  
iQsetup_dhcp.asp   mobiledhcp.asp   natvser.asp     wait.gif       wlwdsenp5.asp  
iQsetup_direct.asp mobiledirect.asp  probe.asp      wan.asp        wol.asp  
iQsetup_dns.asp    mobiledns.asp    quick_timezone.asp wanddns.asp    wpsconfig.asp  
iQsetup_end.asp    mobileend.asp    quick_wan.asp   wandns.asp  
iQsetup_error.asp  mobileerror.asp  stadhcptbl_lanpage.asp wanqosadd.asp  
iQsetup_main.asp   mobilemain.asp  staslog.asp     wanqos.asp
```

Real world case

```
[~/Security/Firmware/BR_6430nS/BR-6430nS_v1.15/squashfs-root/web]> ls  
ezqos.asp          iQsetup_pppoe1.asp    mobilepppoe1.asp    stasylog.asp      wanwisp.asp  
file               iQsetup_pppoe.asp     mobilepppoe.asp    status.asp       wladvance.asp  
FUNCTION_SCRIPT    iQsetup_prob.asp     mobileprob.asp     style.css        wlbasic.asp  
fwcontrol.asp      iQsetup_static1.asp   mobilestatic1.asp syspasswd.asp    wlcontrol.asp  
fwdmz.asp         iQsetup_static.asp    mobilestatic.asp  sysrm.asp       wlencrypt.asp  
fwdos.asp         iQsetup_wireless.asp  mobilewireless.asp systimezone.asp wlschedule.asp  
fwmain.asp        javascript.js       mp.asp           tlcon.asp       wlstatbl.asp  
fwurlb.asp        lan.asp            natalg.asp        tlreset.asp     wlsurvey2.asp  
iQsetup.asp        language.asp       natmain.asp       tlreset_inner.htm wlsurvey.asp  
iQsetup_check.asp  mobilecheck.asp    natpfw.asp       tlupgrade.asp   wlwdsenp3.asp  
iQsetup_detect.asp mobiledetect.asp  natupnp.asp      tlupgrade_inner.asp wlwdsenp4.asp  
iQsetup_dhcp.asp   mobiledhcp.asp    natvser.asp      wait.gif       wlwdsenp5.asp  
iQsetup_direct.asp mobiledirect.asp  probe.asp       wan.asp        wol.asp  
iQsetup_dns.asp   mobiledns.asp     quick_timezone.asp wanddns.asp    wpsconfig.asp  
iQsetup_end.asp   mobileend.asp    quick_wan.asp    wandns.asp  
iQsetup_error.asp  mobileerror.asp   stadhcptbl_lanpage.asp wanqosadd.asp  
iQsetup_main.asp   mobilemain.asp   staslog.asp     wanqos.asp
```



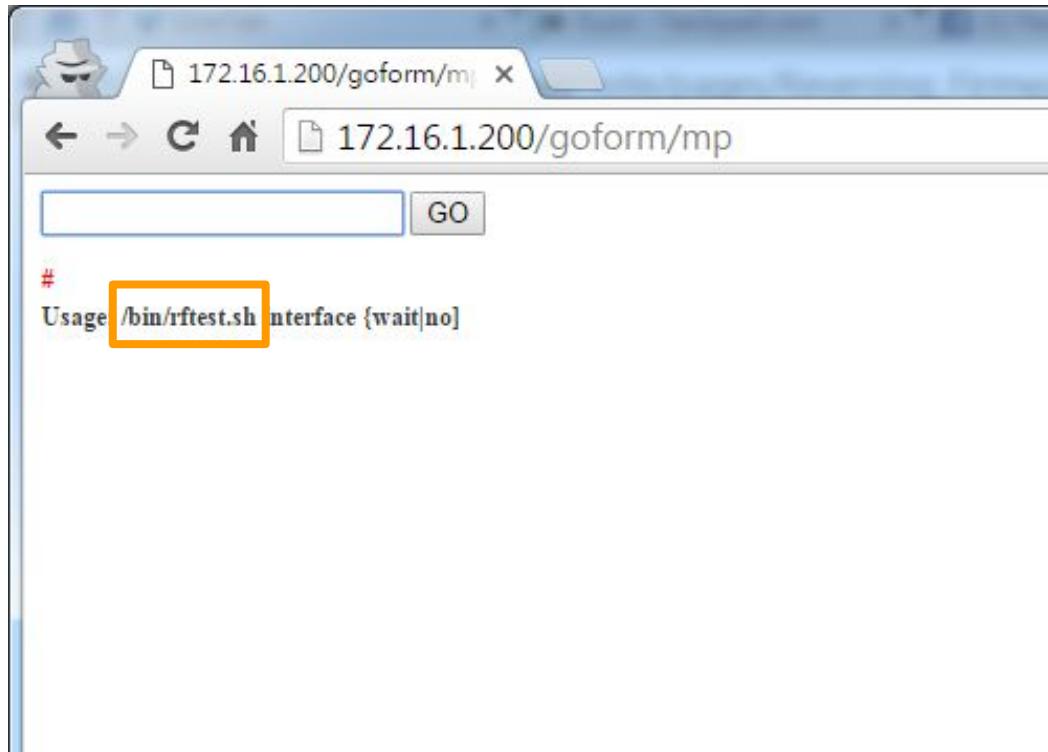
Real world case



Real world case



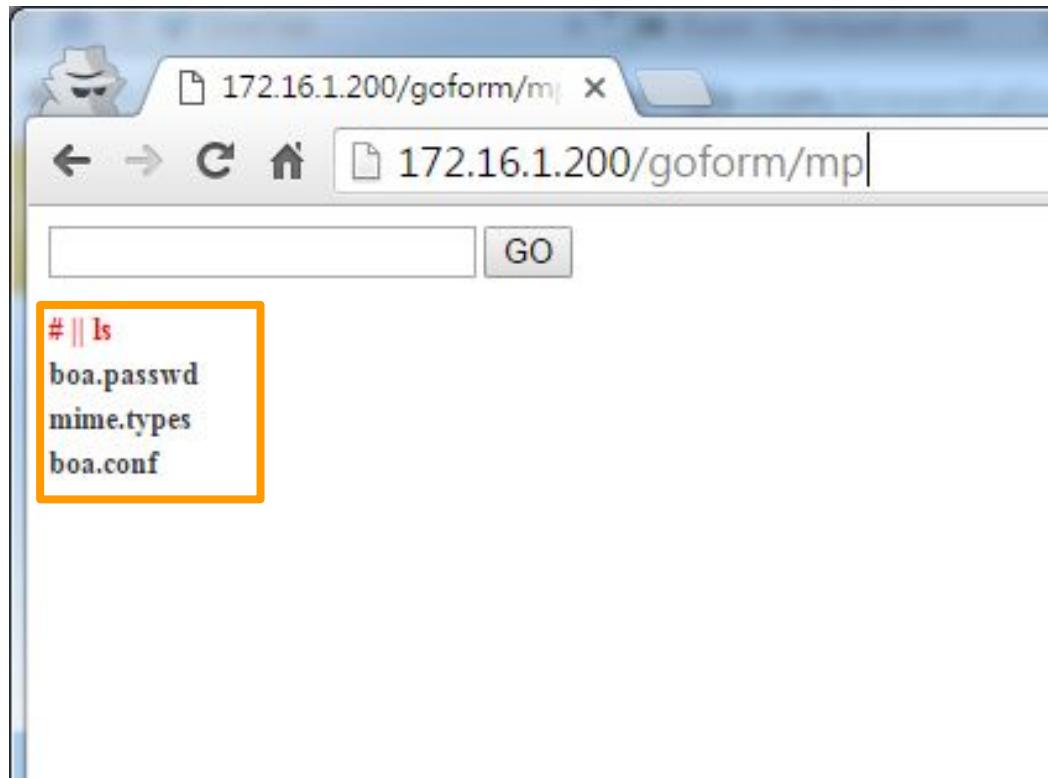
Real world case



Real world case

```
423 ``COMMAND")  
424 if [ "$2" = "ifconfig" ] || [ "$2" = "brctl" ] || [ "$2" = "flash" ] || [ "$2" = "cat" ] || [ "$2" = "echo" ] || [  
    "$2" = "cd" ] || [ "$2" = "sleep" ] || [ "$2" = "kill" ] || [ "$2" = "iwpriv" ] || [ "$2" = "reboot" ] || [ "$2"  
    = "ated" ] || [ "$2" = "AutoWPA" ] || [ "$2" = "iperf" ] ; then  
425 $2 $3 $4 $5 $6  
426 fi  
427 ;;  
428 esac  
NORMAL >> rftest.sh          sh < utf-8[unix] < 100% : 428: 1 <
```

Real world case



Real world case

BusyBox



GPL

Linux內核

軟件版本週期

維基百科，自由的百科全書

BusyBox 是一個遵循[GPL](#)協議、以自由軟體形式發行的應用程式。Busybox在單一的執行檔中提供了精簡的Unix工具集，可執行於多款POSIX環境的作業系統，例如Linux（包括Android^{[6][7][8][9]}）、Hurd^[10]、FreeBSD^{[11][12]}等等。由於BusyBox執行檔尺寸小、並通常使用[Linux內核](#)，這使得它非常適合使用於嵌入式系統。此外，由於BusyBox功能強大，因此有些人將BusyBox稱為「嵌入式Linux的瑞士軍刀」。^[13]

Real world case

範例

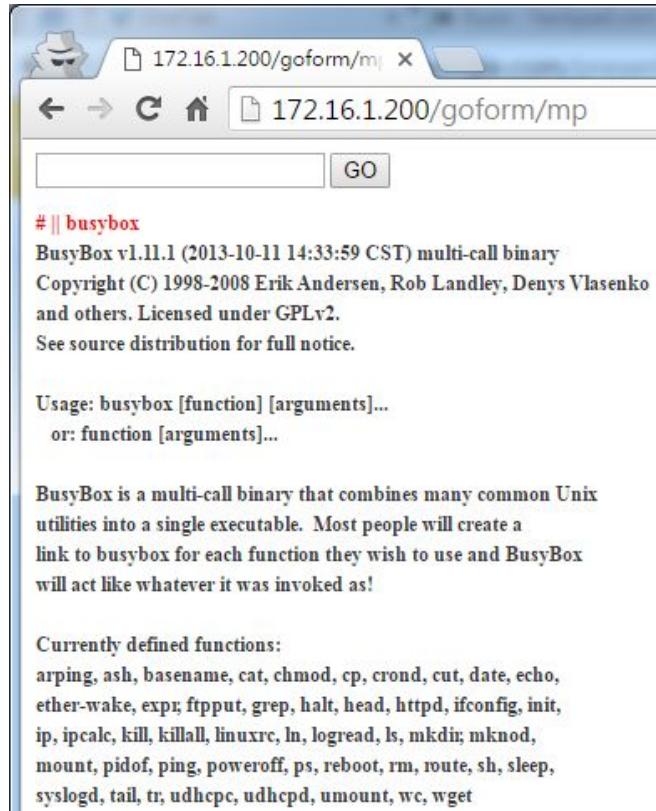
BusyBox 所包含的程式只需要簡單的將名稱附加在第一個參數即可執行：

```
/bin/busybox ls
```

更常見的作法是，這些指令會以連結 (使用硬連結 (英語：hard link) 或者符號連結) 至 BusyBox 可執行檔，BusyBox 會偵測其被連結時的名稱，並執行對應的指令。舉例來說，只要將 `/bin/ls` 連結到 `/bin/busybox`，即可執行

```
/bin/ls
```

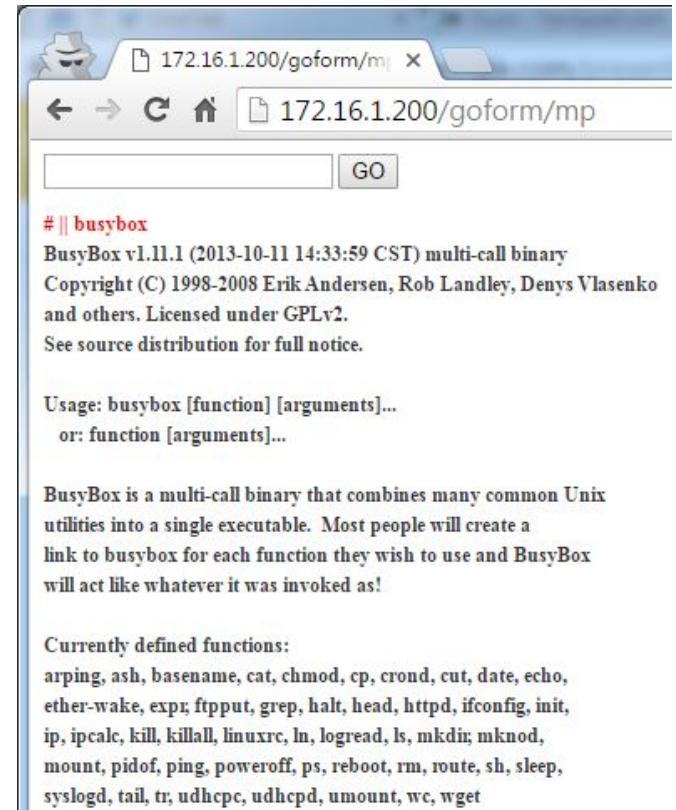
Real world case



Real world case

Currently defined functions:

arping, ash, basename, cat, chmod,
cp, **crond**, cut, date, echo, ether-wake,
expr, **ftpput**, grep, halt, head, httpd,
ifconfig, init, ip, ipcalc, kill,
Killall, linuxrc, ln, logread, ls,
mkdir, mknod, mount, pidof, ping,
poweroff, ps, reboot, rm, **route**,
sh, sleep, syslogd, tail, tr,
udhcpc, udhcpd, umount, wc, **wget**



The screenshot shows a web browser window with the URL `172.16.1.200/goform/mp`. The page displays theBusyBox v1.11.1 (2013-10-11 14:33:59 CST) multi-call binary. Copyright (C) 1998-2008 Erik Andersen, Rob Landley, Denys Vlasenko and others. Licensed under GPLv2. See source distribution for full notice.

Usage: busybox [function] [arguments]...
or: function [arguments]...

BusyBox is a multi-call binary that combines many common Unix utilities into a single executable. Most people will create a link to busybox for each function they wish to use and BusyBox will act like whatever it was invoked as!

Currently defined functions:

```
arping, ash, basename, cat, chmod, cp, crond, cut, date, echo, ether-wake, expr, ftpput, grep, halt, head, httpd, ifconfig, init, ip, ipcalc, kill, killall, linuxrc, ln, logread, ls, mkdir; mknod, mount, pidof, ping, poweroff, ps, reboot, rm, route, sh, sleep, syslogd, tail, tr, udhcpc, udhcpd, umount, wc, wget
```

Real world case

- For debug == For hacker

Real world case

- For debug == For hacker
- After that ?

Real world case

Shodan

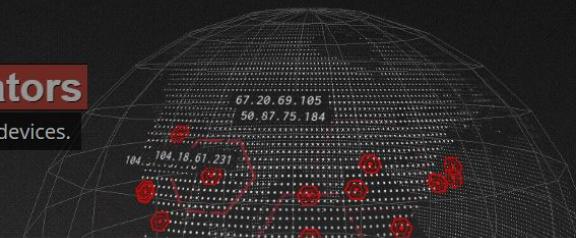
Shodan Developers Book View All...  Explore Enterprise Access Contact Us New to Shodan? Login or Register

SHODAN

The search engine for Refrigerators

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started



Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

Real world case

Censys

About Search Reports API Raw Data Login

 Search ▾

Censys is a search engine that allows computer scientists to ask questions about the devices and networks that compose the Internet. Driven by Internet-wide scanning, Censys lets researchers find specific hosts and create aggregate reports on how devices, websites, and certificates are configured and deployed. [more information]

Real world case

Zoomeye

The screenshot shows the Zoomeye search interface. At the top, there is a navigation bar with links for "搜索", "视角", "海盗榜", "API", and "更多". On the right side of the bar are "注册账号" and "登录" buttons. The main area features a large globe with a network of blue and red dots representing hosts and connections. A search bar at the top of the globe interface contains the query "app:oecms". Below the search bar are two buttons: "探索一下" (Search) and "高级搜索" (Advanced Search). A small tip at the bottom left of the globe says "Tip: Shift + / 可以调出快捷帮助". The Zoomeye logo, which is a stylized eye icon with the text "ZoomEye", is located in the upper left quadrant of the globe's surface.

What is SOHO Router

Firmware overview

Reversing engineering

Common vulnerabilities

Real world case

UCCU

UCCU

problems you may encounter

UCCU

problems you may encounter

- different version, different output ?

UCCU

problems you may encounter

- different version, different output ?
- new stuff or old stuff ?

You may have heard about . . .

You may have heard about . . .

關於 HITCON CTF 的那些事

之 Web 犬如何在險惡的 CTF 世界中存活？

(**CENSORED!**)

This is just beginning . . .

A scene from Game of Thrones featuring the Night King. He is a pale, white-skinned man with blue glowing eyes, wearing a full suit of dark, chainmail-like armor. His arms are outstretched wide, palms up, in a commanding pose. The background is a cold, snowy landscape with other figures in dark cloaks visible in the distance.

IoT is coming

IoT is coming . . .

- SOHO Router

IoT is coming . . .

- SOHO Router
- Web Cam

IoT is coming . . .

- SOHO Router
- Web Cam
- Car

IoT is coming . . .

- SOHO Router
- Web Cam
- Car
- anything smart device

IoT is coming . . .

- SOHO Router
- Web Cam
- Car
- anything smart device
- anything Internet-connected



Questions ?