EMBA

Firmware security analyzer

Michael Messner, Pascal Eckmann

https://github.com/e-m-b-a
@securefirmware

whoami

Michael Messner

Penetration tester
Firmware analysis
Hardware analysis
Siemens Energy AG

@s3curity_de
https://github.com/m-1-k-3
@ michael.messner@siemens-energy.com

whoami

Pascal Eckmann

Cybersecurity Engineer
Security Research
Siemens AG

@_p4cx
https://github.com/p4cx
@ pascal.eckmann@siemens.com

The landscape

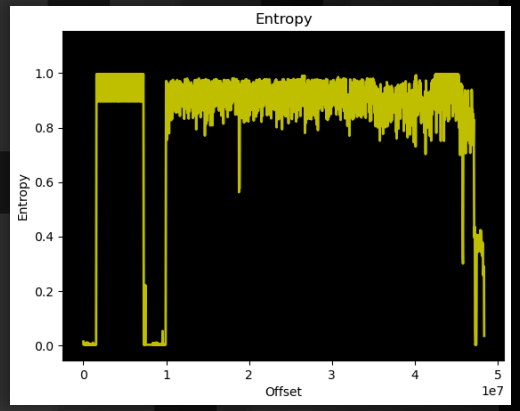
What the firmware analysis

- Firmware is the operating system
- Linux analysis techniques can be used quite often and are well known
- Commercial tools are available, but they are expensive and limited
- EMBA has no limits, costs no money and gives the best results

The typical workflow

- Do some *strings*
- Do some *binwalk*
- Do some *find*
- Do some *regex*
- Do a lot google
- Load something into IDA/Ghidra
- Do something

```
vlan2hwname=et0
pppoe2_flag_Smin=0
wlan_acl_mac6=
wlan_acl_mac7=
wl0_hw_rxchain=1
wlan_acl_mac8=
http_passwd=password
wl_wpa_psk=ap_d-link44
http_rmstartip=0.0.0.0
bpa_passwd=
pptp_localip=0.0.0.0
wlan_acl_mac9=
```




```
┌──(m1k3㉿kali2020-04)-[~/git-repos/sniffROM]
└─$ binwalk output.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
30964         0x78F4          LZMA compressed data, properties: 0x5D, dictionary size: 65536 bytes, un
compressed size: 195236 bytes
131072        0x20000         TRX firmware header, little endian, image size: 3047424 bytes, CRC32: 0x
BE9437E2, flags: 0x0, version: 1, header size: 28 bytes, loader offset: 0x1C, linux kernel offset: 0x9
2EEC, rootfs offset: 0x0
131100        0x2001C         LZMA compressed data, properties: 0x5D, dictionary size: 65536 bytes, un
compressed size: 1658880 bytes
732908        0xB2EEC         Squashfs filesystem, little endian, non-standard signature, version 3.0,
 size: 2443177 bytes, 653 inodes, blocksize: 65536 bytes, created: 2013-04-19 09:04:43
3964944       0x3C8010        gzip compressed data, maximum compression, from Unix, last modified: 197
0-01-01 00:00:00 (null date)
```

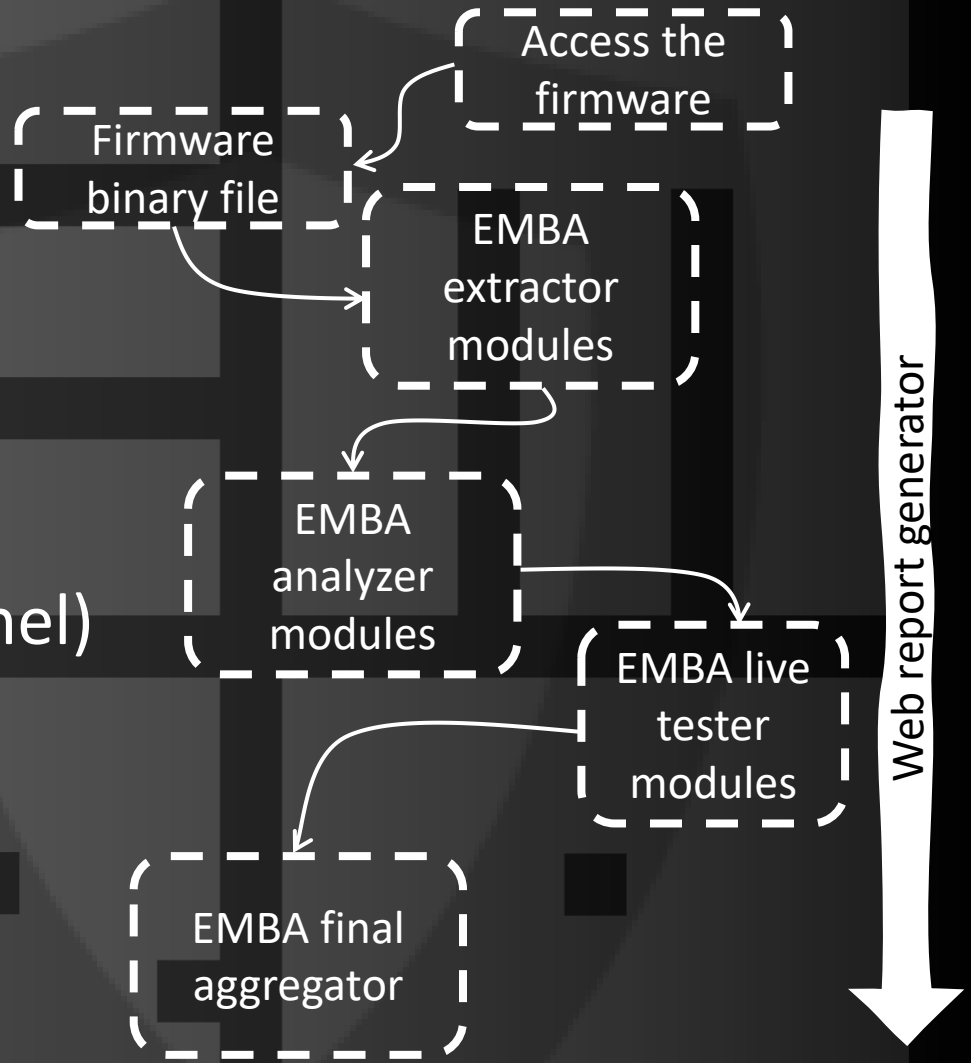
EMBA to the rescue

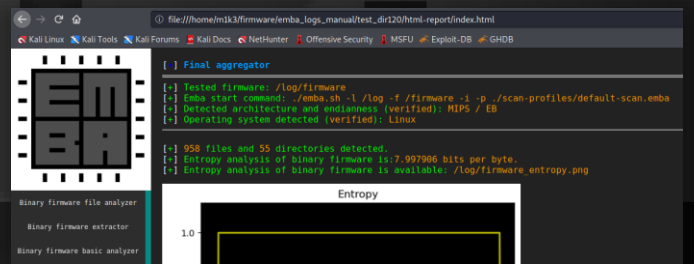
Get the firmware (vendor, hardware)

Extract the firmware (e.g., Linux filesystem, Kernel)

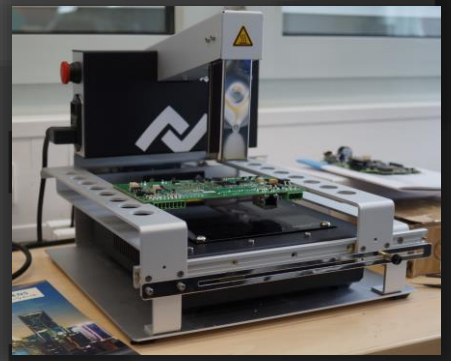
Analyze the firmware

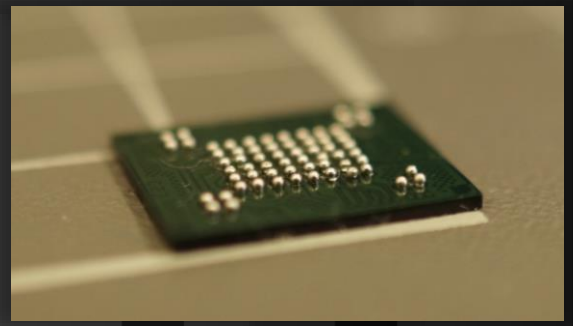
Report all the things



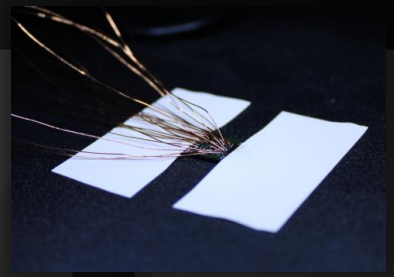


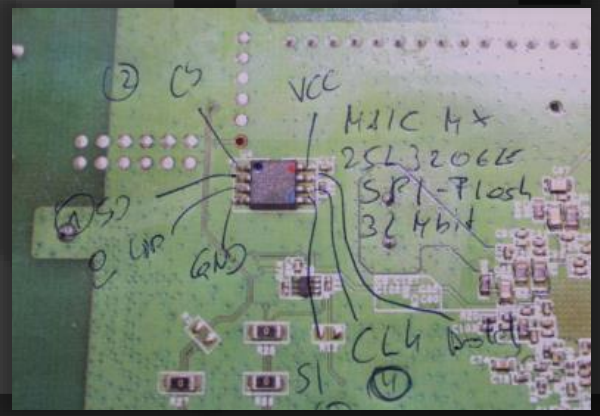
Get the firmware





- Updates from vendor / web site
- Shell access – copy the filesystem via scp, ftp, tftp, nc or to storage device
- Other vulnerabilities e.g., command injection
- JTAG / SWD
- Communication sniffing (e.g., SPI)
- Desolder Flash memory and extract the content

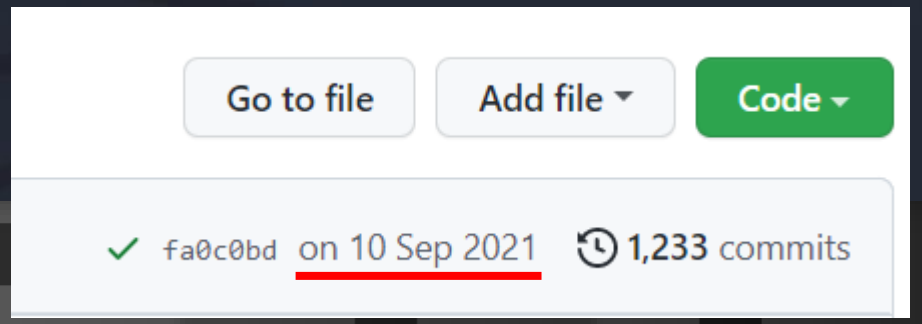




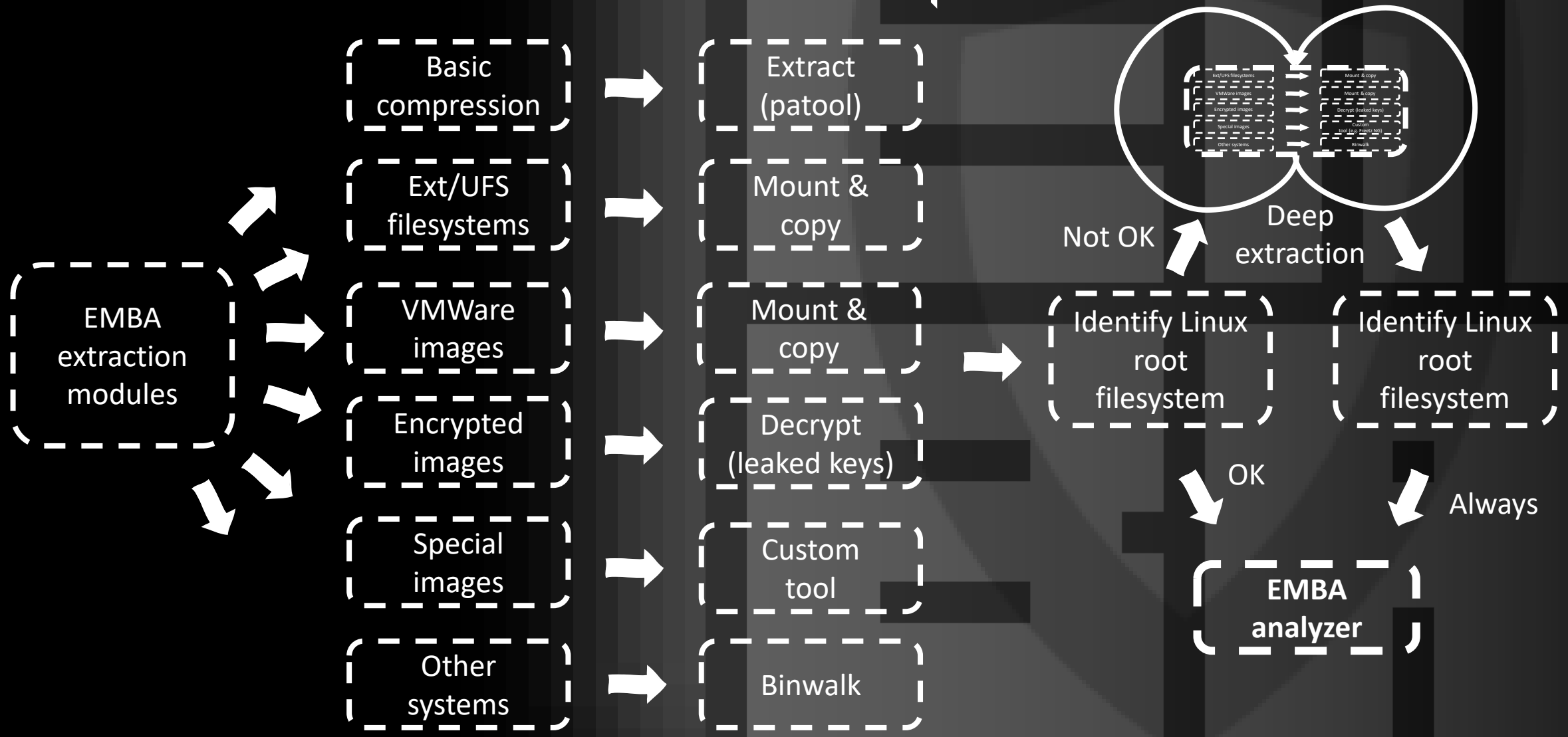
The easiest way

Binwalk all the things

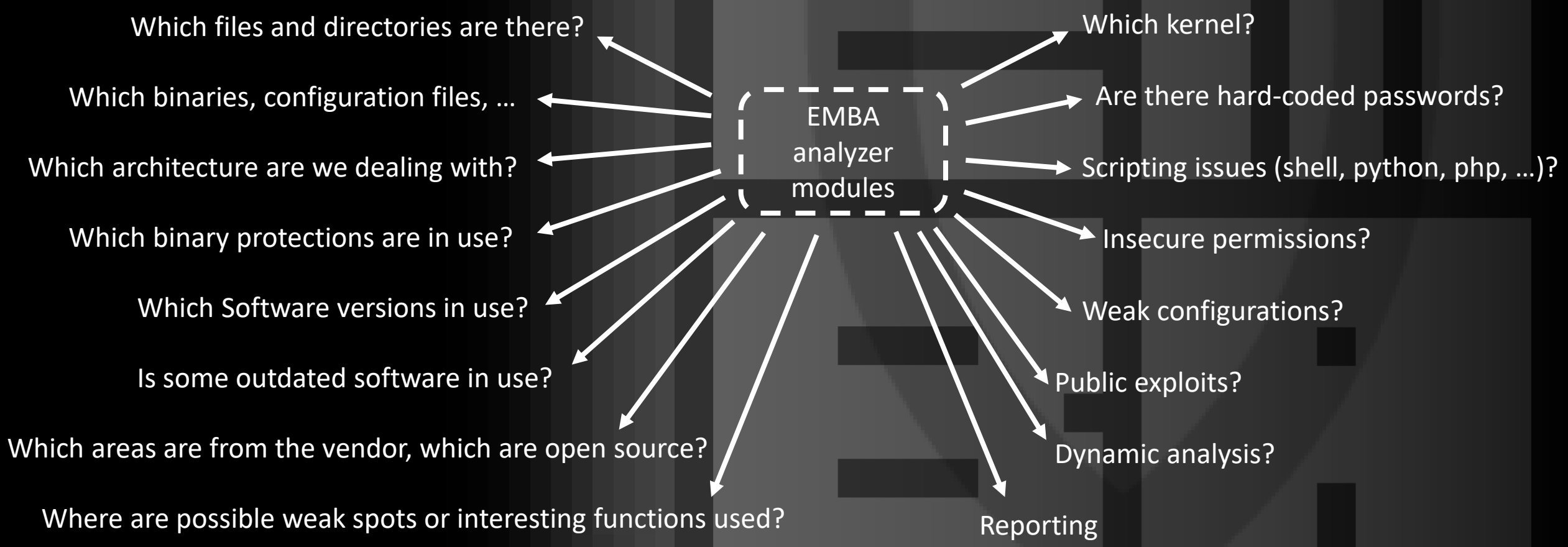
```
┌──(m1k3㉿kali202103)-[~/git-repos/testimages]
└─$ binwalk -e DIR300B5_FW214WWB01.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             DLOB firmware header, boot partition: "dev=/dev/mtdblock/2"
108           0x6C            LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, uncompressed size: 3479564 bytes
1179756       0x12006C        PackImg section delimiter tag, little endian size: 10495232 bytes; big endian size: 2465792 bytes
1179788       0x12008C        Squashfs filesystem, little endian, version 4.0, compression:lzma, size: 2463195 bytes, 1479 inodes, blocksize: 131072 bytes,
6 06:18:46

┌──(m1k3㉿kali202103)-[~/git-repos/testimages]
└─$ ls _DIR300B5_FW214WWB01.bin.extracted/squashfs-root
bin  dev  etc  home  htdocs  lib  mnt  proc  sbin  sys  tmp  usr  var  www

┌──(m1k3㉿kali202103)-[~/git-repos/testimages]
└─$
```



The EMBA extraction process



Finally, we have something extracted



Don't reinvent the wheel

Multiple Linux tools
binwalk
Freetz-NG
Checksec.sh
CVE and CVSS databases
CVE-Search
CVE-Searchsploit
cwe-checker
GHIDRA

Docker
Radare2
fdtdump
linux-exploit-suggester
OpenSSL
uboot mkimage
objdump
pixd
bandit
progpilot

Qemu
shellcheck
sshdcc
tree
unzip
sudo parser
sshdc
Yara
and others …

See also: https://github.com/e-m-b-a/emba/wiki/Installation#dependencies

Hunting 0days

Identify interesting spots

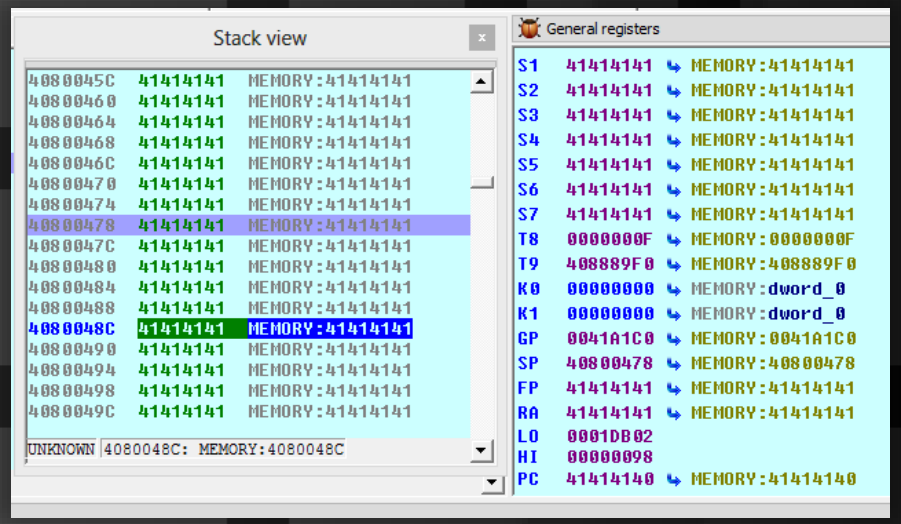
What the 0day?

- 0day – unknown vulnerability (There is no patch available)
  - You have to find the vulnerability by yourself
  - The goal of every penetration tester is to find 0days

- 1day – already known vulnerability (Patches are in the [illegible] available)
  - You have to identify the components with exact version details (SBOM) and match it against a vulnerability database
  - The goal of every penetration tester is to do this automagically and do not waste time with it
  - It is also an interesting thing for developers, security teams and the purchasing department

Weak binary functions

When using legacy C functions such as strcpy, it's up to the developer to make sure the size of the buffer to be written to is large enough to avoid buffer overruns. If this is not done properly, it can result in a buffer overflow, causing the program to crash at a minimum. At worst, a carefully crafted overflow can cause malicious code to be executed.



Source: https://rules.sonarsource.com/c/RSPEC-1081

Identify interesting spots

Create disassembly

objdump

radare2

Weak fct counter

Check network functionality

Check binary protection mechanisms

Common Linux file

```
585254:     8fbc0028     lw      gp,40(sp)
585258:     27b104e4     addiu   s1,sp,1252
58525c:     8f99a15c     lw      t9,-24228(gp)
585260:     02202021     move    a0,s1
585264:     0320f809     jalr    t9
585268:     27a50728     addiu   a1,sp,1832
58526c:     8fbc0028     lw      gp,40(sp)
585270:     2684a87c     addiu   a0,s4,-22404
```

```
[+] Found 498 (88%) binaries without enabled stack canaries in 563 binaries.
[+] Found 536 (95%) binaries without enabled RELRO in 563 binaries.
[+] Found 22 (3%) binaries without enabled NX in 563 binaries.
[+] Found 211 (37%) binaries without enabled PIE in 563 binaries.
[+] Found 537 (95%) stripped binaries without symbols in 563 binaries.
```

```
628   : ncc            : common linux file: no
67    : wscd           : common linux file: no
60    : libupnp.so.1.3. : common linux file: no
36    : busybox        : common linux file: yes
35    : libuClibc-0.9.2 : common linux file: no
32    : minidlna       : common linux file: yes
21    : iptables       : common linux file: yes
20    : ip6tables      : common linux file: yes
14    : ntfs-3g        : common linux file: yes
14    : miniupnpd      : common linux file: no
```

Identify interesting spots

```
[+] Found 3042 usages of strcpy in 324 binaries.

[+] STRCPY - top 10 results:
    1576  : setup.cgi       : common linux file: no   |  No RELRO  |  No Canary  |  NX disabled  |  No Symbols  |  No Networking    |
    244   : setupwizard.cgi : common linux file: no   |  No RELRO  |  No Canary  |  NX disabled  |  No Symbols  |  No Networking    |
    96    : rc_apps         : common linux file: no   |  No RELRO  |  No Canary  |  NX disabled  |  No Symbols  |  Networking       |
    95    : minidlna        : common linux file: yes  |  No RELRO  |  No Canary  |  NX disabled  |  No Symbols  |  Networking       |
    84    : zip             : common linux file: yes  |  No RELRO  |  No Canary  |  NX disabled  |  No Symbols  |  No Networking    |
    57    : busybox         : common linux file: yes  |  No RELRO  |  No Canary  |  NX disabled  |  No Symbols  |  Networking       |
    51    : leafp2p         : common linux file: no   |  No RELRO  |  No Canary  |  NX disabled  |  No Symbols  |  Networking       |
    44    : afpd            : common linux file: no   |  No RELRO  |  No Canary  |  NX disabled  |  No Symbols  |  Networking       |
    34    : iptables-multi  : common linux file: no   |  No RELRO  |  No Canary  |  NX disabled  |  No Symbols  |  No Networking    |
    32    : libuClibc-0.9.3 : common linux file: no   |  RELRO     |  No Canary  |  NX disabled  |  Symbols     |  No Networking    |

[+] SYSTEM - top 10 results:
    236   : rc_apps         : common linux file: no   |  No RELRO  |  No Canary  |  NX disabled  |  No Symbols  |  Networking       |
    216   : setup.cgi       : common linux file: no   |  No RELRO  |  No Canary  |  NX disabled  |  No Symbols  |  No Networking    |
    202   : scfgmgr         : common linux file: no   |  No RELRO  |  No Canary  |  NX disabled  |  No Symbols  |  Networking       |
    152   : setupwizard.cgi : common linux file: no   |  No RELRO  |  No Canary  |  NX disabled  |  No Symbols  |  No Networking    |
    114   : multi_pb_app    : common linux file: no   |  No RELRO  |  No Canary  |  NX disabled  |  No Symbols  |  No Networking    |
    105   : wizard          : common linux file: yes  |  No RELRO  |  No Canary  |  NX disabled  |  No Symbols  |  Networking       |
    101   : generate_cert_f : common linux file: no   |  No RELRO  |  No Canary  |  NX disabled  |  No Symbols  |  No Networking    |
    95    : led_switch      : common linux file: no   |  No RELRO  |  No Canary  |  NX disabled  |  No Symbols  |  No Networking    |
    93    : dnrd            : common linux file: no   |  No RELRO  |  No Canary  |  NX disabled  |  No Symbols  |  Networking       |
    91    : httpd_watchdog  : common linux file: no   |  No RELRO  |  No Canary  |  NX disabled  |  No Symbols  |  No Networking    |
```

See also: https://flattsecurity.medium.com/finding-bugs-to-trigger-unauthenticated-command-injection-in-a-netgear-router-psv-2022-0044-2b394fb9edc by @stereotype32

The 1day issue

What the 1day?

- 0day – unknown vulnerability (There is no patch available)
  - You have to find the vulnerability by yourself
  - The goal of every penetration tester is to find 0days

- 1day – already known vulnerability (Patches are in theory available)
  - You have to identify the components with exact version details (SBOM) and match it against a vulnerability database
  - The goal of every penetration tester is to do this automagically and do not waste time with it

What's the problem?!?

- We are working on the compiled/packed firmware
- Mostly no source code with component versions available
- No standardised format of version details
- No standardised mechanism/parameter on how to get version details

```
└$ bash --version
GNU bash, Version 5.1.4(1)-release
Copyright (C) 2020 Free Software Fo
```

```
└$ openssl version
OpenSSL 1.1.1k  25 Mar 2021
```

```
└$ perl -V
Summary of my perl5 (revision 5 version 32 subversion 1) configuration:
```

Hybrid version detection in EMBA

Static analysis

Dynamic analysis

Output generation with string analysis, kernel modules, path details

Output generation with Qemu

EMBA database with version identifiers

Version detection in EMBA

Match the output against a version dictionary:

```
[+] Version information found BusyBox v1.12.1  in binary /bin/busybox (license: gplv2) (emula
[+] Version information found BusyBox v1.12.1 (2013-12-11 14:05:50 CST) multi-call binary in
[+] Version information found BusyBox v1.12.1 (2013-12-11 14:05:50 CST) in binary /bin/busybo
[+] Version information found Dnsmasq version 2.41 in binary /sbin/dnsmasq (license: gplv3) (
[+] Version information found Easy Cast du Multi Hub (ecmh) 2005.02.09 by Jeroen Massar <jero
[+] Version information found igmpproxy, Version 0.1 in binary /bin/igmpproxy (license: unkno
[+] Version information found ip6tables v1.4.10 in binary /bin/ip6tables (license: unknown) (
[+] Version information found iptables v1.4.10 in binary /bin/iptables (license: gpl) (emulat
[+] Version information found iproute2-ss110107 in binary /bin/ds (license: gplv2) (emulation
[+] Version information found iptables v1.4.10 in binary /bin/iptables (license: gpl) (emulat
[+] Version information found iwevent   Wireless-Tools version 29 in binary /bin/iwevent (lic
[+] Version information found iwconfig  Wireless-Tools version 29 in binary /bin/iwconfig (li
```

```
[*] Software inventory initial overview:
[+] Found Version details (statical check): busybox:1.12.1
[+] Found Version details (statical check): dnsmasq:2.41
[+] Found Version details (statical check): gnu:sed:4.0
[+] Found Version details (statical check): igmpproxy:0.1
[+] Found Version details (statical check): libpcap:1.0.0
[+] Found Version details (statical check): mailsend:1.15b5
[+] Found Version details (statical check): mini_httpd:1.19
[+] Found Version details (statical check): minidlna:1.0.25
[+] Found Version details (statical check): miniupnpd:1.7
[+] Found Version details (statical check): openssl:0.9.8e
[+] Found Version details (statical check): pppoe-discovery:3.3
[+] Found Version details (statical check): samba:3.0.24
[+] Found Version details (statical check): udhcp:1.12.1
[+] Found Version details (statical check): zlib:1.2.3
[+] Found Version details (statical check): zlib:1.2.5
[+] Found Version details (emulator): busybox:1.12.1
[+] Found Version details (emulator): dnsmasq:2.41
[+] Found Version details (emulator): ecmh:2005.02.09
[+] Found Version details (emulator): igmpproxy:0.1
[+] Found Version details (emulator): iproute2:110107
[+] Found Version details (emulator): iptables:1.4.10
[+] Found Version details (emulator): mailsend:1.15b5
[+] Found Version details (emulator): mini_httpd:1.19
[+] Found Version details (emulator): minidlna:1.0.25
[+] Found Version details (emulator): mtd-utils:1.1.1.1
[+] Found Version details (emulator): ntfs-3g:2012.1.15
[+] Found Version details (emulator): openssl:0.9.8e
[+] Found Version details (emulator): point-to-point_protocol:2.4.4
[+] Found Version details (emulator): pppoe-discovery:3.3
[+] Found Version details (emulator): ralink-dot1x:2.6.0.0
[+] Found Version details (emulator): rdnssd:1.0.1
[+] Found Version details (emulator): roaring_penguin:pppoe:3.10
[+] Found Version details (emulator): udhcpc:0.9.9
[+] Found Version details (emulator): watchdog:5.6
[+] Found Version details (emulator): wireless_tools:29
[+] Found Version details (emulator): xlink:15.0
[+] Found Version details (kernel): kernel:2.6.36
```

We love exploits

```
samba                    :      3.0.24          :      CVE-2012-1182    :      10.0     :      Exploit (EDB ID: 21850 (R) / MSF: setinfopolicy_heap (R) / Github:
amisha  ial-az_Week16-Homework (G) esteban0477_RedTeamPlaybook (G) Eutectico_Steel-Mountain (G) Juba0x4355_Blue-Writeup (G) katgoods_week16 (G) notsag-dev_htb-blu
e (G)  ag-dev_htb-legacy (  rogram-smith_THM-Blue (G) Qft  ormation_Collection_Handbook (G) superhero1_OSCP-Prep (G))
samba                    :      0.24            :      CVE-20   46      :      10.0     :      Exploit (EDB ID: 9950 (R) / MSF: lsa_addprivs_heap (D) lsa_transnam
es_heap (  sa_transnames_h  (R) lsa_transnames_heap (R) lsa_  snames_heap (R) / Github: DOCTOR-ANR_cybercaptor-server (G) fiware-cybercaptor_cybercaptor-serv
er (G) Larryxi_My_tools (G)  dongliang_LinuxFlaw (G) oneoy_cve- (
kernel                   :      2.6.36          :      CVE-2017-7895    :      10.0     :      Exploit (Github: thdusdl1219_CVE-Study (G))
kernel                   :      2.6.36          :      CVE-2016-9555    :      10.0     :      Exploit (Github: thdusdl1219_CVE-Study (G))
kernel                   :      2.6.36          :      CVE-2016-7117    :      10.0     :      Exploit (Github: R0B1NL1N_linux-kernel-exploitation (G) skbasava_Li
nux-Kernel-exploit (G) Technoashofficial_kernel-exploitation-linux (G) thdusdl1219_CVE-Study (G) xairy_linux-kernel-exploitation (G))
kernel                   :      2.6.36          :      CVE-2016-3955    :      10.0     :      Exploit (Github: pqsec_uboatdemo (G) thdusdl1219_CVE-Study (G))
kernel                   :      2.6.36          :      CVE-2016-10229   :      10.0     :      Exploit (Github: thdusdl1219_CVE-Study (G))
kernel                   :      2.6.36          :      CVE-2016-10150   :      10.0     :      Exploit (Github: thdusdl1219_CVE-Study (G))
kernel                   :      2.6.36          :      CVE-2015-8812    :      10.0     :      Exploit (Github: thdusdl1219_CVE-Study (G))
kernel                   :      2.6.36          :      CVE-2015-8787    :      10.0     :      Exploit (Github: sriramkandukuri_cve-fix-reporter (G) thdusdl1219_C
VE-Study (G))
kernel                   :      2.6.36          :      CVE-2015-1421    :      10.0     :      Exploit (Github: thdusdl1219_CVE-Study (G))
samba                    :      3.0.24          :      CVE-2020-1472    :      9.3      :      Exploit (EDB ID: 49071 (R) / MSF: cve_2020_1472_zerologon / Github:
0x727_usefull-elevation-of-privilege (G) 0xcccc666_cve-2020-1472_Tool-collection (G) 0xkami_CVE-2020-1472 (G) 0xsyr0_OSCP (G) 0xT11_CVE-POC (G) 422926799_CVE-2020-
1472 (G) 61106960_adPEAS (G) aasphixie_aasphixie.github.io (G) alexverboon_MDATP (G) alphaSeclab_sec-daily-2020 (G) aRustyDev_C844 (G) Ascotbe_Kernelhub (G) Astrog
eorgeonethree_Starred (G) b4rtik_SharpKatz (G) bb00_zer0dump (G) BC-SECURITY_Invoke-ZeroLogon (G) bhassani_Recent-CVE (G) bhdresh_SnortRules (G) bjknbrrr_PENTESTIN
G-BIBLE (G) blaCCkHatHacEEkr_PENTESTING-BIBLE (G) B-nD_report (G) boh_RedCsharp (G) bollwarm_SecToolSet (G) CanciuCostin_CVE-2020-1472 (G) CasperGN_ActiveDirectory
```

```
[+] WARNING: Vulnerability CVE-2021-22600 is a known exploited
[+] WARNING: Vulnerability CVE-2019-13272 is a known exploited
[+] WARNING: Vulnerability CVE-2016-5195 is a known exploited
```

```
[*] Exploitability notes:
    R - remote exploits
    L - local exploits
    D - DoS exploits
    G - PoC code found on Github (unknown exploit vector)
    X - Vulnerability is known as exploited
```

Version detection in EMBA

```
[*] Identified the following software inventory, vulnerabilities and exploits:
[+] Found version details:  sed                  :  4.0          :  CVEs: 0      :  Exploits: 0
[+] Found version details:  igmpproxy            :  0.1          :  CVEs: 0      :  Exploits: 0
[+] Found version details:  ecmh                 :  2005.02.09   :  CVEs: 0      :  Exploits: 0
[+] Found version details:  busybox              :  1.12.1       :  CVEs: 13     :  Exploits: 3
[+] Found version details:  dnsmasq              :  2.41         :  CVEs: 23     :  Exploits: 17
[+] Found version details:  iproute2             :  110107       :  CVEs: 0      :  Exploits: 0
[+] Found version details:  iptables             :  1.4.10       :  CVEs: 1      :  Exploits: 0
[+] Found version details:  libpcap              :  1.0.0        :  CVEs: 5      :  Exploits: 0
[+] Found version details:  mailsend             :  1.15b5       :  CVEs: 0      :  Exploits: 0
[+] Found version details:  mini_httpd           :  1.19         :  CVEs: 3      :  Exploits: 2
[+] Found version details:  minidlna             :  1.0.25       :  CVEs: 0      :  Exploits: 0
[+] Found version details:  mtd-utils            :  1.1.1.1      :  CVEs: 0      :  Exploits: 0
[+] Found version details:  miniupnpd            :  1.7          :  CVEs: 5      :  Exploits: 2
[+] Found version details:  ntfs-3g              :  2012.1.15    :  CVEs: 22     :  Exploits: 1
[+] Found version details:  point-to-point_proto :  2.4.4        :  CVEs: 4      :  Exploits: 1
[+] Found version details:  pppoe-discovery      :  3.3          :  CVEs: 0      :  Exploits: 0
[+] Found version details:  ralink-dot1x         :  2.6.0.0      :  CVEs: 0      :  Exploits: 0
[+] Found version details:  rdnssd               :  1.0.1        :  CVEs: 0      :  Exploits: 0
[+] Found version details:  pppoe                :  3.10         :  CVEs: 0      :  Exploits: 0
[+] Found version details:  udhcp                :  1.12.1       :  CVEs: 0      :  Exploits: 0
[+] Found version details:  udhcpc               :  0.9.9        :  CVEs: 0      :  Exploits: 0
[+] Found version details:  openssl              :  0.9.8e       :  CVEs: 82     :  Exploits: 28
[+] Found version details:  wireless_tools       :  29           :  CVEs: 0      :  Exploits: 0
[+] Found version details:  watchdog             :  5.6          :  CVEs: 0      :  Exploits: 0
[+] Found version details:  samba                :  3.0.24       :  CVEs: 47     :  Exploits: 11
[+] Found version details:  xlink                :  15.0         :  CVEs: 0      :  Exploits: 0
[+] Found version details:  zlib                 :  1.2.3        :  CVEs: 0      :  Exploits: 0
[+] Found version details:  zlib                 :  1.2.5        :  CVEs: 0      :  Exploits: 0
[+] Found version details:  kernel               :  2.6.36       :  CVEs: 1496   :  Exploits: 500
[+] Identified 29 software components with version details.

[+] Identified 1701 CVE entries.
    Identified 417 High rated CVE entries / Exploits: 175
    Identified 936 Medium rated CVE entries / Exploits: 286
    Identified 348 Low rated CVE entries /Exploits: 91
    553 possible exploits available (23 Metasploit modules).
    Remote exploits: 9 / Local exploits: 63 / DoS exploits: 69 / Github PoCs: 512
```

EMBA

Firmware security analyzer

Michael Messner, Pascal Eckmann

https://github.com/e-m-b-a
@securefirmware

@ pascal.eckmann@siemens.com @ michael.messner@siemens-energy.com