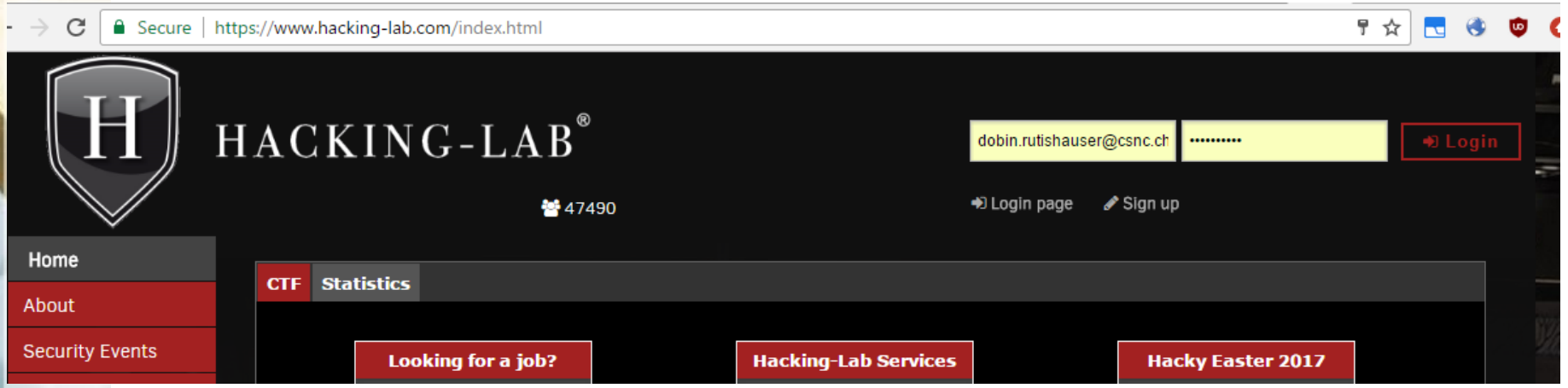
Yookiterm – http://exploit.courses

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

Tel +41 55 214 41 60
Fax +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Yookiterm: Exploit.courses

Yookiterm: Exploit.courses

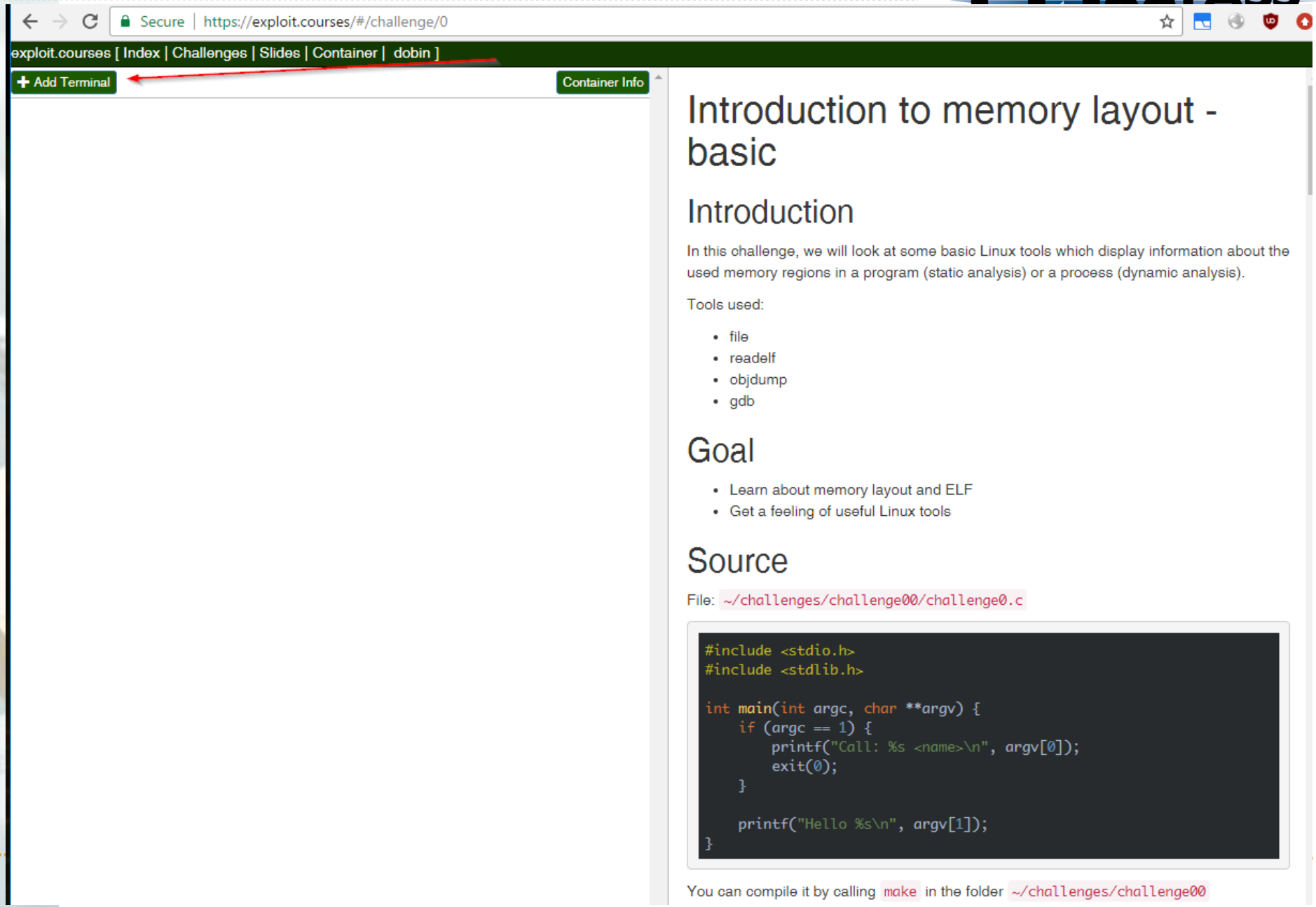


exploit.courses: Challenges

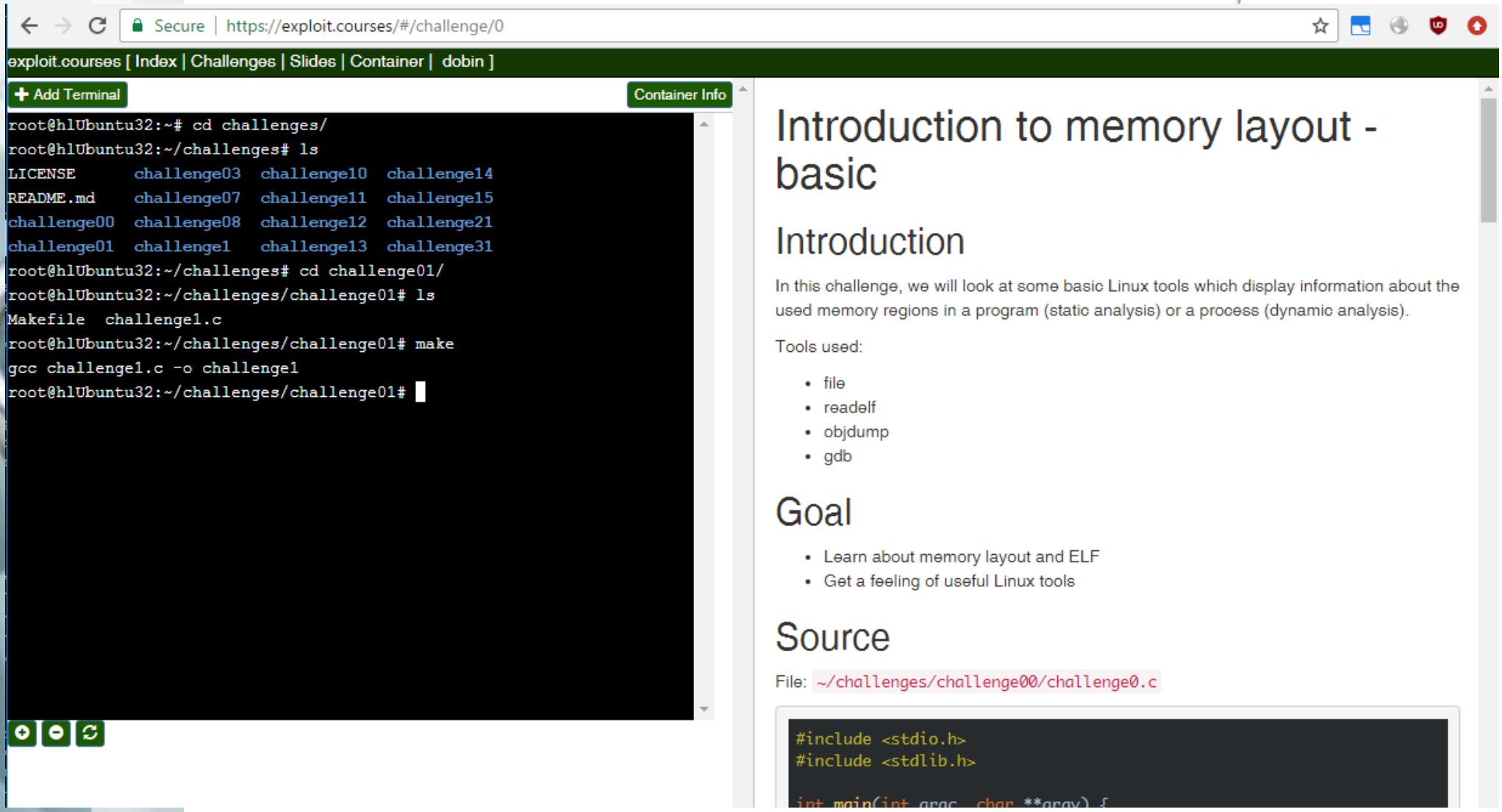
exploit.courses [Index | Challenges | Slides | Container | dobin]

ID	Title	Description	Arch	Bits	ASLR
0	Introduction to memory layout - basic	Static and dynamic analysis of an ELF binary with Linux command line tools	intel	32	✔
1	Introduction to memory layout - advanced	Research on where the different types of variables are stored in an ELF file	intel	32	✔
3	Introduction to shellcode development	Create a basic running shellcode (print to console)	intel	32	✖
7	Function Call Convention in x86 (32bit)	Analysis of function calling (gdb static and dynamic analysis)	intel	32	✖
8	C buffer analysis	Analysis of out-of-bound read with gdb	intel	32	✖
10	Simple Buffer overflow	Overwrite local variables on the stack to bypass authentication	intel	32	✖
11	Development of a buffer overflow exploit - 32 bit	How to create a simple buffer overflow exploit	intel	32	✖
12	Development of a buffer overflow exploit - 64 bit	How to create a simple buffer overflow exploit	intel	64	✖
13	Development of a remote buffer overflow exploit - 64 bit	How to create a buffer overflow exploit for a networked server	intel	64	✖
14	Stack canary brute force	How to brute force the stack canary in a remote server	intel	64	✖
15	Development of a remote buffer overflow exploit - 64 bit with ASLR	How to create a contemporary remote buffer overflow exploit	intel	64	✔
20	Introduction to ARM	Basics of the ARM architecture	arm	32	✔
21	Introduction to develop an ARM buffer overflow	Create a simple buffer overflow on ARM	arm	32	✔
31	Heap use-after-free analysis	Analyse a simple use-after-free bug in noteheap	intel	64	✔
50	Introduction to GDB	A reference and playground for GDB	intel	32	✖

exploit.courses: Challenges



exploit.courses: Challenges



exploit.courses: Container

There are three different container you can access:

- ASLR (32, 64 bit)
- NO ASLR (32, 64 bit)
- ARM (32, 64 bit)

32 and 64 bit hosts are usually shared, including data

exploit.courses: Container

Container lifetime: 6 days

Container max lifetime: 12 days

Copy your files with SCP

exploit.courses: Container

The challenge files (vulnerable programs, exploits):

- https://github.com/dobin/yookiterm-challenges-files

The challenge writeups:

- https://github.com/dobin/yookiterm-challenges