# pkgsrcCon 2018 kgsrc July 6<sup>th</sup> to 8<sup>th</sup> 2018 Berlin, Germany https://pkgsrc.org/pkgsrcCon/2018/

## Sequel to London 2017

- Thanks Sevan for a smooth conference!
- And inspiring us for prepping this one

#### Welcome to the c-base!

- Space station under Berlin
- There is space for all of us
- Contact your gentle organizers for any issue:
  - @docscream <tm@core.io>
  - @khorben <khorben@defora.org>
     (and for any feedback)

### About the c-base

- Some say it is the mother of all hackerspaces
- It was there before the word existed
- Reconstructing the station since 1995 in Berlin
- Main hall and terrace as public areas
- The bar will open intermittently later
- Possibly a tour of the member area later?

#### Internet access

- Open wireless networks:
  - c-base-public
  - c-base-public-5ghz
  - freifunk-cbase
- Reminder: no encryption!

In alphabetical order...

#### This venue



Shirts & badges defora networks

## Catering



#### **Travel & accommodation**



## About shirts and badges

- Shirt for everyone */at the time of printing/* 
  - 3 M, 4 L, 4 XL for the first registrations
  - Re-print possible (contact khorben)
- Badge 3D-printed at khorben's home factory
  - Re-print possible too (same thing)

## Arrival day

- At the Republik Berlin
- How was it?

#### Talks

10:15	Hugo Teso	Keynote
11:00	Youri Mouton	The state of desktops in pkgsrc
12:00	Amitai Schleier	Maintaining qmail in 2018
14:00	Maya Rashish	A beginner's introduction to GCC
15:00	Leonardo Taccari	Handling the workflow of pkgsrc-security
16:00	Benny Siegert	Preaching for pkgsrc-releng
17:00	Sevan Janiyan	Something old, something new, something borrowed

#### Talks

- The talks will be recorded and posted online
- Streaming was not confirmed by the time I prepared these slides

## Lunch

- Pizza from Papa Pane!
- Possibly the best in Berlin
- Sponsored by SkyLime
- Most of them vegetarian-friendly
- Specific needs please tell us \*now\*

## Social dinner

- Burgers at Spud BencerPossibly the best in Berlin
- Burger, fries and a drink
- French place with French cuisine
- Vegetarian and vegan options
- A room for ourselves (at the back)

## Social dinner

- Burgers at Spud BencerPossibly the best in Berlin
- Burger, fries and a drink
- French place with French cuisine
- Vegetarian and vegan options
- A room for ourselves (at the back)

### Social Dinner

- S+U Warschauer Str.
- Ticket: Kurzstrecke (two stops away)
- From S+U Jannowitzbrücke: any eastbound train (S3 S5 S7 S9)
- From Warschauer Str.:
  - Right when exiting, straight until REWE across the street
  - Take the street between REWE and Warschauer Str., Gubener Str. 41
- We can organize a group departure!

## Chillax day

- Same place, same time
- No plan

### Keynote

#### Hugo Teso, author of devel/radare2-cutter

<sup>0</sup> 1 <sup>0</sup> 2 <sup>0</sup> 3 <sup>0</sup> 4 5 <sup>0</sup> 6 7 <sup>0</sup> 8 <sup>0</sup> 9 []= Cutter					°1 °2 <mark>°</mark> 3 °4 5 6 7 8 9 []= /bin/ksh	
File Edit View Windows Help						/bin/ksh 192×27
$ \leftarrow \rightarrow $	Type flag name or address here				140 kamil@rugged /home/kamil # screenfetch -s gnnnOCCCCCObaau,	kamil@rugged
						OS: NetBSD Kernel: and64 NetBSD 8.99.14
					WYXCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC	Karhel: andra rectsu 8.99.14 Uptine: Uh 37n Packages: 773 Shell: ksh Recolution: 3286×1080
Functions	Ø ₩	Hexdump 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF	0 8	Sidebar I Sidebar Side	\W\\xCCCCCCCCCCCCCCCCCCCCCCCCCF"'	Shell: ksh
sym.autu viork2 body	129092 0x0041bf30 c0.0f.85	e 02 00 00 31 c9 48 8d 54 24 30 89 de	Parsing Information		\W\\XCCCCCCCCCCCCCCCCCCCCF"'	Resolution: 3286×1080 MM: dum
sym.atfu_vfork2_head	17 0x0041bf40 bf 26 00 0	0 00 e8 86 5a fe ff 83 f8 ff 0f 84 27 .6Z	Disassembly 👻 Endian Litt 👻	✓ Offset info:	\N\\"PCOCCCOCCFP""	
sym.atfu_vfork3_body	129056 0x0041bf50 03 00 00 8 17 0x0041bf60 00 31 c9 b	b 3d 27 c5 21 00 85 ff 0f 85 84 02 00='.! a 01 00 00 00 89 de bf 07 00 00 00 e8 .1	Arch x86 - Bits 64 -	STACKOP null FAMILY cpu		GIN Thene: Releigh LUKZ] Icon Thene: Releigh Context CPU: Intel Core 17-4650U e 4x 2.2950Hz GPU: Mess DRI Intel(R) Heavell Mobile
sym.atfu_vfork3_head sym.atfu_vfork4_body		f 83 f8 ff 0f 84 27 03 00 00 8b 35 fd \Z		COND al	VII) VII) VIII VIIII VIIII VIIII VIIII VIIII VIIII VIIII VIIII VIIII VIIII VIIII	GPU: Mesa DRI Intel(R) Haswell Mobile
sym.atfu_vfork4_head	17 0x0041bf80 c4 21 00 8	5 f6 0f 85 8a 02 00 00 31 d2 48 8d 74 .!	0x0041bdb3 7842 js	STACK null FAIL 0x0041bdb5	\NN\ \NNN	RNH: 3895MiB / 15799MiB
sym.atfu_vfork5_body	128981 0x0041bfa0 2a 03 00 0	f e8 17 58 fe ff 48 98 48 39 c5 0f 85 \$,XH.H9 0 8b 0d d6 c4 21 00 85 c9 0f 85 53 02 *	0x41bdf7 0x0041bdb4 ???	IUMP 0x0041bdb5	\NNA.	
sym.atfu_vfork5_head	1/ 0x0041bfb0 00 00 31 d	9 31 d2 89 de bf 08 00 00 00 e8 0e 5a1.1Z	0x0041bdb5 ???	ESIL sf,?{,4308471,rip,=,}	NNR,	
sym.atfu_vfork6_body	128945 0x0041bfc0 fe ff 83 1	8 ff 0f 84 3c 03 00 00 8b 15 af c4 21	0x0041bdb6 ???	TYPE cjmp SIZE 2	\NNW\	
sym.atfu_vfork6_head sym.atfu_vfork7_body		f 85 52 02 00 00 31 d2 48 8d 74 24 2cR1.H.t\$, 9 57 fe ff 48 98 48 39 c5 0f 85 b8 03WH.H9	0x0041bdb7 ??? 0x0041bdb8 ???	REFPTR 0	\NNN\	
sym.atfu_vfork7_body sym.atfu_vfork7_head	17 0x0041bff0 00 00 31 0	2 be 09 00 00 00 8b 7c 24 2c e8 ec 5d1	0.0042000	BYTES 7842	Taking shot in 3., 2., 1.,	
sym.atfu vfork8 body	138967 0x0041c000 fe ff 8b 0	5 78 c4 21 00 85 c0 74 11 be df 77 42x.!twB		ID 274		
sym.atfu_vfork8_head	1/ 0×0041c020 8d 74 24 2	7 42 00 31 c0 e8 83 57 fe ff 31 d2 48,w8.1,W1.H c 89 df e8 85 57 fe ff 45 31 c0 83 f8 .ts,WE1	Disassembly 🖉 🗷	<ul> <li>Opcode description:</li> </ul>		
sym.atfu_write_d1_body	1031 0x0041c030 ff 41 0f 9	4 c0 b9 f0 78 42 00 ba 0a 00 00 00 be .AxB	0041c0b6 xor esi, esi	# js:		
sym.atfu_write_d2_body	1224 0x0041c040 37 01 00 0	0 bf 08 e6 42 00 e8 62 58 fe ff 48 81 7BbXH. 0x0	0041c0b8 mov rdi, rbx	jump short if sign (sf=1)		
sym.atfu_write_d3_body sym.atfu_write_d4_body	1605 0x0041c060 0f 85 67 0	1 00 00 31 c9 31 d2 31 f6 31 ff e8 5da1.1.1.1]	0041c0bb call sym.inp.nemset 0041c0c0 nov word [0x5000], 0x4f : '0' : [0x5000:2]=0			/bin/ksh 134x17
svm.atfu x86 64 cve 2018 8897 body	1379 0x0041c070 59 fe ff 8	3 f8 ff 0f 84 18 03 00 00 bf 1c 00 00 Y	0041c0ca nov ebp, dword [obj.debug] ; [0x638480:4]=0		41c0f1: ff 28	ljmp *(%rax)
sym.atfu_x86_64_cve_2018_8897_head	1/ 0-0041-0000 10 10 00 /		0041c0d0 test ebp, ebp			
sym.atfu_x86_64_regs1_body	1643 0x0041c020 00 08 12 5		0041c0d2 jne 0x41c17b 0041c0d8 mov edi, 0x11 ; 17		000000000041c0f3 <farjmp32≻:< td=""><td></td></farjmp32≻:<>	
sym.atfu_x86_64_regs1_head		8 89 c2 31 f6 48 89 df e8 b0 55 fe ff WH1.HU 0x0	0041c0dd call sym.imp.raise		41c0f3: f9	
sym.attach1_raw sym.await zombie raw			0041c0e2 test eax, eax		41c0f4: c0 41 00 73	rolb \$0x73,0x0(%rcx)
sym.can we set dbregs	120 0x0041c0e0 fe ff 85 d	0 0f 85 bc 00 00 00 48 c7 c0 f3 c0 41HA	0041c0e4 jne 0x41c1a6 0041c0ea mov rax, loc.farjmp32 ; 0x41c0f3			
sym.check_happy		9 c0 41 00 73 00 bc 00 50 00 00 17 cd(A.sP 0x0	0041c0f1 ljmp (rax)	<ul> <li>X-Refs to current address:</li> </ul>		
sym.dbregs_dont_inherit_execve			0041c0f3 farjnp32: 0041c0f3 stc	Address Instruction	000000000041c0f9 <trigger32>:</trigger32>	
sym.dbregs_dont_inherit_lwp	2538 0x0041c120 bf 70 76 4	2 00 31 c0 e8 74 56 fe ff e9 66 fd ff .pvB.1tVf	0041c0f4 rol byte (rcx), 0x73		41c0f9: bc 00 50 00 00	mov \$0x5000,%esp
sym.dbregs_trap_variable sym.dsum			.0041c0f8 ~ add byte [rax + rax + 0x17000050], bh		41c0fe: 17	(bad)
sym.dummy fn2			0041c0f9 trigger32: 0041c0f9 mov esp. 0x5000		41c0ff: cd 04	int \$0x4
sym.dummy_fn3	68 0x0041c160 84 5a fd 1	f ff be df 77 42 00 bf e8 77 42 00 31 .ZwBwB.1	0041c0fe invalid		41c101: 8b 1d 79 c3 21 00	mov 0x21c379(%rip),%ebx # 638480 <debug< th=""></debug<>
sym.dummy_fn4			0041c0ff int 4		41c107: 85 db	test %ebx.%ebx
sym.forkee_status_exited	0x0041c190 0c 56 fe 1	f bf 11 00 00 00 e8 52 56 fe ff 85 c0 .VRV	0041c101 mov ebx, dword [obj.debug] ; [0x638480:4]=0 0041c107 test ebx, ebx		41c109: 0f 85 32 01 00 00	jne 41c241 <trigger32+0x148></trigger32+0x148>
sym.forkee_status_stopped sym.impdifftime50	183 0x0041c190 0c 56 fe 0x0041c1a0 0f 84 44	f ff ff 41 b9 54 77 42 00 41 b8 60 26DA.TwB.A.`& 🛛 🛛 🖓 🖓 🖓 🖓 🖉	0041c109 jne 0x41c241		41c10f: bf 05 00 00 00	mov \$0x5,%edi
	0 0x0041c1b0 43 00 b9 0	9 01 00 00 ba 08 e6 42 00 be f8 73 42 CBsB 0x0 0 00 00 31 c0 e8 33 56 fe ff e8 8e 5413VT 0x0	0041c10f nov edi, 5 0041c114 call sym_imp, exit	<ul> <li>X-Refs from current address:</li> </ul>	41c114: e8 17 55 fe ff	callg 401630 <_exit@plt>
sym.imperrno	0x0041c1d0 fe ff 89 d	6 bf e0 76 42 00 31 c0 e8 c0 55 fe ffvB.1U	0041c114 call sym.impexit 0041c119 call sym.imp.getpid	Address Instruction		carrd across (Textrebre)
sym.implibc_thr_yield		f ff bf 68 78 42 00 e8 41 57 fe ff 90hxBAW	0041clle mov esi, eax	Address Instruction		
sym.impsigaction14	0x0041c200 e9 32 fd 1	f ff bf 00 e8 42 00 e8 31 57 fe ff 90 .lBlW f ff bf 52 e8 42 00 e8 21 57 fe ff 90 .2R.BlW	Þ			
sym.impsigprocmask14	0 (0x0041c210 e9 9d fd 1	f ff be df 77 42 00 bf e8 77 42 00 31wBwB.1				
sym.impstat50	6 (*) 0x0041c220 c0 e8 7a 5	5 fe ff e9 60 fd ff ff be df 77 42 00zU`wB. 2 00 31 c0 e8 64 55 fe ff e9 98 fd ffwB.1dU				
sym.impsyscall	0x0041c240 ff bf 90 3	7 42 00 e8 e5 56 fe ff e9 bf fe ff ffwBV				
sym.imptime50	6 🕑 🔤 0x0041c250 e8 9b 53 1	e ff 8b 38 e8 e4 56 fe ff 49 89 c0 b9S8VI				
orm impsearch1.4		0 ba a6 76 42 00 be f8 00 00 00 bf 08 .vBvBvB.				
Quick Filter	X Dashboard Graph (sym.atfu_	(86_64_regs1_body) Hexdump Pseudocode Entry Points Strings	Imports Symbols Notepad			
Entry Points			Sections	88		
> Analysis finished	Name	<ul> <li>Size Address End Address</li> </ul>		· · · ·		
> Populating UI	.bss	0 0x006382a0 0x00638a40				
> Finished, happy reversing :)	.com			<b>T</b>		
To remove this message, put `dbxenv suppres	s startup message 7.5' in your .dbxrc 📃 .ctor					
	data					
	.dtor	16 0x00637e58 0x00637e68		· · ·		

#### Keynote

#### The stage is yours!