https://ctftime.org/event/854/

Chaos Communication Camp 2019

星期五, 23 八月 2019, 10:00 UTC — 星期日, 25 八月 2019, 10:00 UTC

On-line

A Chaos Communication Camp event.

Format: Jeopardy

Official URL: https://camp.allesctf.net/

This event's weight is subject of public voting!

Rating weight: 0

Event organizers

- ALLES!

0

ALLES is looking forward to host this year's Camp CTF, which will be held during the Chaos Communication Camp 2019 in Ziegeleipark Mildenberg. This Jeopardy style CTF is open to everyone and can be played online.

Scoreboard

358 teams total

Place	Team	CTF points	Rating points*
1	sf	4150.000	0.000
2	RedRocket	3987.000	0.000
3	OpenToAll	3548.000	0.000
4	RPISEC	3462.000	0.000
5	dcua	2588.000	0.000

6	cockmasters	2351.000	0.000
7	Shellphish	2048.000	0.000
8	MELTDOWN	1976.000	0.000
9	GoN	1654.000	0.000
10	KuK Hofhackerei	1398.000	0.000
11	mode13h	1178.000	0.000
12	ENOFLAG	1130.000	0.000
13	JBZ	1074.000	0.000
14	FireShell	1074.000	0.000
15	C4T BuT S4D	1057.000	0.000
16	TeamPowerPrinter	995.000	0.000
17	lesglandus	953.000	0.000
18	spritzers	948.000	0.000
19	Cyberlandsholdet	948.000	0.000
20	jinmo123	924.000	0.000
21	Dragon Sleep Pwn Sector	837.000	0.000
22	coldnorth	765.000	0.000
23	the cr0wn	754.000	0.000
24	Jinotega	750.000	0.000
25	flexerilla	749.000	0.000
26	Team {insert name here}	710.000	0.000
27	dqi	658.000	0.000
28	Pham Solo 2	633.000	0.000
29	0x90r00t	632.000	0.000
30	Hecării, Țuica și Păunii	558.000	0.000
31	Contrail	551.000	0.000
32	Delusions of Grandeur	551.000	0.000
33	technic	542.000	0.000
34	HackingForSoju	528.000	0.000
35	NeoRaider	468.000	0.000
36	Zeus WPI	429.000	0.000
37	cyber	429.000	0.000
38	vitol3ss	427.000	0.000
39	KITCTF	427.000	0.000

40	zer0pts	421.000	0.000
41	saarsec	421.000	0.000
42	🐠	412.000	0.000
43	HeroKenzan	412.000	0.000
44	OPPvFgbB2Lx6OSa	412.000	0.000
45	watevr	410.000	0.000
46	luxeria	386.000	0.000
47	doubV	379.000	0.000
48	BitWornHats	379.000	0.000
49	kasia-tutej	331.000	0.000
50	quriosity	331.000	0.000
51	Bigos	311.000	0.000
52	Code Cabana	311.000	0.000
53	InfoSecIITR	305.000	0.000
54	Tinfoil Hats	296.000	0.000
55	SealTeam1	296.000	0.000
56	Kernel Sanders	294.000	0.000
57	Banditter i Habitter	289.000	0.000
58	Team Pancakes	289.000	0.000
59	shellrippers	289.000	0.000
60	0x1	287.000	0.000
61	TeamRocketIst	287.000	0.000
62	onotch	287.000	0.000
63	PwnablePandas	287.000	0.000
64	TahSec	287.000	0.000
65	TheShittyBeatles	268.000	0.000
66	UiO-CTF	262.000	0.000
67	ácaros	251.000	0.000
68	Lycan$	246.000	0.000
69	kuro	246.000	0.000
70	sh!tware	221.000	0.000
71	burner_herz0g	221.000	0.000
72	n0n3	208.000	0.000
73	_gh0st_	204.000	0.000

74 Blue Hens 204.000 0.000
75 PGiatasti 204.000 0.000
76 ssh@uzl 204.000 0.000
77 rootGrant 204.000 0.000
78 M30W 204.000 0.000
79 badfirmware 204.000 0.000
80 lol lol 197.000 0.000
81 Mars Explorer 197.000 0.000
82 ClaraConquersAlles 197.000 0.000
83 warlock_rootx 197.000 0.000
84 HillHackers 197.000 0.000
85 room2042 178.000 0.000
86 Vanshal Gaur 178.000 0.000
87 PWNsticciotti 171.000 0.000
88 e.g. 171.000 0.000
89 hoc 171.000 0.000
90 /dev/base 171.000 0.000
91 TMHC 171.000 0.000
92 Spikers 171.000 0.000
93 K1_W4L0 171.000 0.000
94 Pilou44 171.000 0.000
95 PoE 171.000 0.000
96 M.I.S.T. 171.000 0.000
97 bora9 171.000 0.000
98 kanbedon 171.000 0.000
99 hAIXer 171.000 0.000
100 noplalic 171.000 0.000

Crypto========

Power

Category: Crypto

Difficulty: Easy

Author: black-simon

First Blood: RedGKFRocket

RSA is to boring. Raise to the power of x instead.

power.py download http://static.allesctf.net/power-7919baccbb5643b6bf263d5f026709e6030980a15c3d6b49ef1eb5b52c0ee64a.py

nc hax.allesctf.net 1337

Prejudiced Randomness 1

Category: Crypto

Difficulty: Easy/Medium

Author: Th0mas

First Blood: RedGKFRocket

I found new uber crypto that allows us to securely generate random numbers! Lets use this to play a very fair game of random chance. Win the game!

```
nc hax.allesctf.net 7331
```

challenge.py download https://static.allesctf.net/prejudiced-2d332bfde033d72af2c04293710c90de7da93c1240b9e821810747dc9c195667.py

Prejudiced Randomness 2

Category: Crypto

Difficulty: Hard

Author: Th0mas

First Blood: RedGKFRocket

Since this game is random, losing should be just as easy as winning, right?

```
nc hax.allesctf.net 7331
```

challenge.py https://static.allesctf.net/prejudiced-2d332bfde033d72af2c04293710c90de7da93c1240b9e821810747dc9c195667.py

licpwn1

Category: Crypto

Difficulty: Easy/Medium

Author: 0x4d5a

First Blood: dcua

You found this cool service and really want to buy a flag. A real flag! That would totally make your day. Unfortunately, the real flags are sold out. Find a way to get the flag anyway.
Note: licpwn stage2 can only be solved once stage1 has been solved.
hax.allesctf.net:8888

Forensics========

FlagConverter Part 1

Category: Forensics

Difficulty: Easy

Author: TheVamp

First Blood: Sudovoodoo

On the campground of the CCCamp, someone is trying to troll us by encrypting our flags. Sadly, we only got the memory dump of the PC which encrypted our flags.
Please provide us with the flag which is not yet encrypted.
flagconverter.7z https://static.allesctf.net/flagconverter-725b6d252230016c8126c5d972760e08b824f8a86071e87aa52e6f069a2e18f3.7z

FlagConverter Part 2

Category: Forensics

Difficulty: Medium

Author: TheVamp

First Blood: cockmasters

On the campground of the CCCamp, someone is trying to troll us by encrypting our flags. Sadly, we only got the memory dump of the PC which encrypted our flags.
Please decrypt the flag for us which was encrypted a few seconds ago.

FlagConverter Part 3

Category: Forensics

Difficulty: Medium/Hard

Author: TheVamp

First Blood: sf

On the campground of the CCCamp, someone is trying to troll us by encrypting our flags. Sadly, we only got the memory dump of the PC which encrypted our flags.
We know that a third flag is still missing.
Could you find the last flag for us, please?

kuchenblech3

Category: Forensics

Difficulty: Medium

Author: localo & A2nkF

The mafia is using CS:GO to communicate secretly. They are talking about some "flag" but we don't know what to look for. We managed to intercept parts of their communication. Can you make some sense out of this and get this "flag"?
traffic.pcap https://static.allesctf.net/kuchenblech3-traffic-a3aa3b38db4b7feed305e6574daa3edf3d36deaefb73677e794dd6f27fb45f5e.pcap

Hint 1: The original filename was `31_07_2019.pcap`

Misc========

Ancient Data

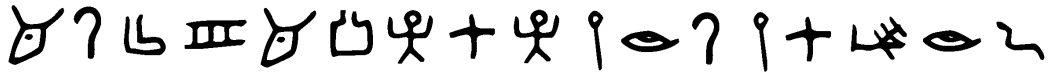
Category: Misc

Difficulty: Easy (Google the world)

Author: TheVamp

First Blood: 0x90r00t

That is some ancient stuff! Could you translate that for us?



Put your translated text in the following format, to submit the Flag: ALLES{<translated text>}

Sanity Check

Category: Misc

Difficulty: Sanity Check

Author: CherryWorm

First Blood: DDot

Pay our IRC channel a visit :^)

babyquantum

Category: Misc

Difficulty: Medium/Hard

Author: CherryWorm

First Blood: RedGKFRocket

Our engineers have been hard at work the last couple of weeks, creating the quantum Accelerated Linear Logic Enumeration Solver (qALLES). This one of a kind quantum computer has a unique never seen before quantum gate, which uses a special secret. Can you leak this secret?

hax.allesctf.net:5000

Pwn========

Keychain

Category: Pwn

Difficulty: Premium (i.e. really hard)

Author: LinHe

We've found parts of the source code of a keychain backdoor that has been installed by Kim Jong-un's Agents on Donald Trump's computer. As we're interested in getting Trump's Twitter password, we would like you to find out what the backdoor does and how it can be exploited.

The source code can be found here. https://static.allesctf.net/keychain-4feee5145575351a2741ba4a70ba30618d4397c0.zip

Once you got a working exploit, please:

- Send an IRC message to LinHe with a URL to your exploit and
- Call Linus: Extension: AAPL (2275) or wait

Hints:

- The source code is for a program that patches something in securityd.
- The patcher is not that interesting - Just pretend this is macOS <= 10.14.3 but find a different mach port over-deallocation vulnerability.
- The flag can be found in the keychain. It is a standard `Internet Password`with the Name/Account set to `@realdonaldtrump`. (Or just dump the whole keychain)
- This or this might help you. https://youtu.be/wPd6rMk8-gg https://objectivebythesea.com/v2/talks/OBTS_v2_Henze.pdf
- Our VM is running macOS 10.14.6 (i.e. the latest version of macOS).
- The VM is not connected to the internet.
- You will need to find a 0day.

core-pwn

Category: Pwn

Difficulty: Easy/Medium

Author: 0x4d5a

First Blood: OpenToAll

We heard the .NET framework is secure and stuff. Nothing can go wrong, it's a memory safe language! Really. Nothing.

Built with `dotnet publish --runtime ubuntu.18.04-x64` and executed in a docker container: `FROM mcr.microsoft.com/dotnet/core/aspnet:2.1.12-bionic`

`nc hax.allesctf.net 1234`

core-pwn.zip https://static.allesctf.net/core-pwn-9562bd3d1d641e90e3b86b8525b636d71ddd91d2.zip

hsmprototype

Category: Pwn

Difficulty: Hard

Author: Kun (external) & explo1t

First Blood: Shellphish

You scanned the interwebz for vuln boxes and suddenly:

A wild HSM prototype appeared...

By chance you also found the binary behind the service, but it only contains a PLACEHOLDER masterkey! Can you recover the real key?

Server at: hsm.allesctf.net 4321 (Server currently very unstable, if you wanna work on it online, contact explo1t in irc to get a private instance)

Hint 1: You can now download a modified qemu version, in which you can run the firmare on your host

firmware-474e4cf3bb0d53cedadf1f884679d186d5a737c4a9be4258b6f210aba2785381.zip

qemu-fbf326ac045e3a9dc3362fe5451b0ed93d8912120da4587258bf2b91c116b4eb.zip

(Build instructions: ./configure && make -j4)

(Run with: ./startdemo.sh connect to the service with telnet localhost 4321 for example)

licpwn2

Category: Pwn

Difficulty: Medium/Hard

Author: 0x4d5a

Dependencies: licpwn1

Solve licpwn1 for details.

pwning your kernelz

Category: Pwn

Difficulty: 0day

Author: LinHe

This time we got a real macOS kernel 0day for you! And the bug is super easy to trigger:

```
x86_saved_state32_t state;
memset(&state, 0xFF, sizeof(x86_saved_state32_t));
thread_set_state(mach_thread_self(), x86_SAVED_STATE32,
(thread_state_t) &state, x86_SAVED_STATE32_COUNT);
while (1) {}
```

Please exploit it to become root. Flag can be found in `/flag`.

Source code and the kernel we're using can be found here.

https://static.allesctf.net/pwning_your_kernelz-5feee5145575351a2741ba4a70ba30618d4397c0.zip

Once you got a working exploit, please:

- Send an IRC message to LinHe with a URL to your exploit and
- Call Linus: Extension: AAPL (2275) or wait

Hints:

- This bug can only be exploited by 32 bit apps, therefore you will need Xcode 9.4.1 or lower.
- We're running the latest version of macOS, 10.14.6.

- The included kernel is the development kernel from the latest KDK.
- You will need to disable SMAP on your mac. This is why we use the development kernel: You can disable SMAP like this (only possible with development kernels): `sudo nvram boot-args="-pmap_smap_disable"`
- SMEP is enabled. The kernel slide will be passed to your exploit in the first argument as hex string (i.e. we will run your program like this: `./exploit 0xDEADBEEF` with 0xDEADBEEF being the kernel slide).
- Our VM is not connected to the internet.

regfuck

Category: Pwn

Difficulty: Medium/Hard

Author: localo

First Blood: RedGKFRocket

Unlimited free `Hello World`s at `hax.allesctf.net:3301`.

Ubuntu 18.04

regfuck.zip https://static.allesctf.net/regfuck-a3031b02792dfd4eb68835e486d36f0a95bca60f896b5514b1b1e59b26f5cd8a.zip

Note: The server is LD_PRELOADing buffer_read.so to mitigate a short read. You can ping us on IRC if this causes issues with your exploit.

https://static.allesctf.net/buffer_read-5fe18e81c36930c00edf04bb6d10ca74a74fbd7aefd79dd2870dd57498bfb28c.so

Radio========

Garage

Category: Radio

Difficulty: Hard

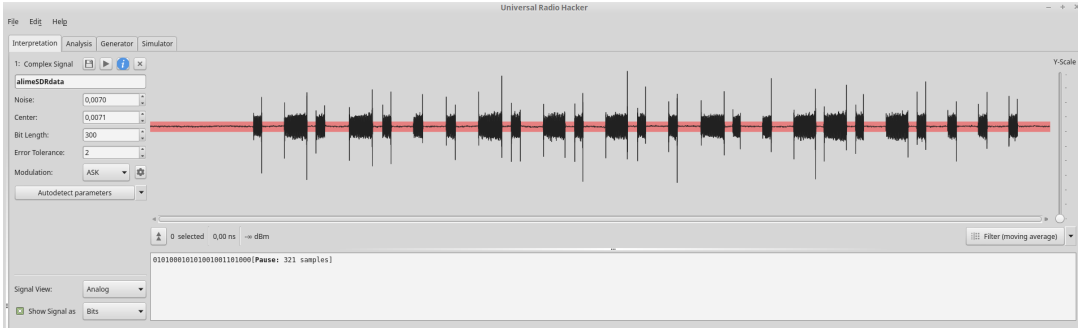
Author: explo1t

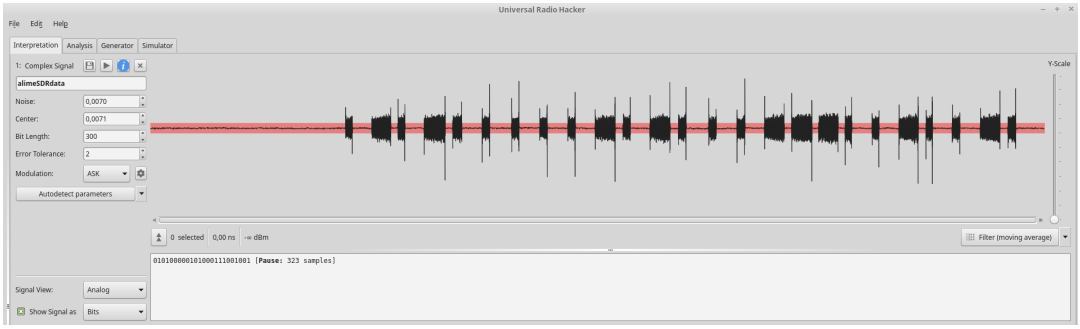
First Blood: Dragon Sleep Pwn Sector

In order to safeguard their flags, the ALLES team has brought their secure storage garages to the camp. They can be opened remotely with transmitters, using military-grade encryption™. We heard about security issues with similar products, but according to the manufacturer, their garages are secure! Phew.
Only a small number of highly trusted team members carry the transmitters. Unfortunately, one of them got drunk on Tschunk and a transmitter for one of the garages ended up in enemy hands.
You got hold of the remote control and can press the button:http://hax.allesctf.net:8080
Can you raid the second flag vault?
The following parameters might help you:

- Symbol Duration: 512u
- Sample Rate: 200k
- Frequency: 433.920 MHz

The signal is transmitted near Dragon Sleep Pwn Sector (each signal 10 times, bc transmission errors). You can either connect to our remote receiver, or receive the signal locally using the SDR of your choice. For transmitting your solution, please use our submission queue which will allocate a time slot, transmit your signal and provide you with a video feed of the garage.
You cannot physically access the garages.
Update: Contact explo1t on IRC if you believe you have a working exploit.
Update2: New client with increase performance. Increased disconnection time, if no ping (now 120s).
Hint 1: Here is a full Challenge-Response from Garage 1 (The one you can open via the webinterface)





Hint 2: Challenge Message Format:

2Bit Garage ID

5Bit Rolling Code (minutes%30)

101010 Static

11Bit Random (static until challenge solved)

Remote transceiver: garage-e9cfbc3da45f4dd32c3ce3e98e141422830a8460d10a44e8388be53e27e13e41.zip

Reverse Engineering========

CampRE

Category: Reverse Engineering

Difficulty: Easy/Medium

Author: 0x4d5a

First Blood: dcua

.NET Core is strange. There is no executable, but i'm sure you'll find a way to execute the file anyway. The remaining part of the challenge should be easy :)

CampRE.zip https://static.allesctf.net/CampRE-a18ff98bf94e11c2646f01b36c6b2850537a75a4.zip

Update1: We noticed that not every user has a 1337 core CPU and lowered the calculation power a little bit. Should be even more fun now! Please redownload the file.

WillNotCry

Category: Reverse Engineering

Difficulty: Easy/Medium

Author: Informator

First Blood: cockmasters

Your company was confronted with the truth of a ransomware that encrypted precious files. Unfortunately, the backup is only moved to cold-storage once a day. The newest backup of the password database is encrypted.

Find the flag in the newest password database backup.

https://static.allesctf.net/willnotcry-77fb268e55113fdd96e9de432fa0553cbf28cf2c2c8a2aed0f32206ff4cd2da1.tar.gz

Systems / Network========

Enterprise DevOps 1

Category: Systems / Network

Difficulty: Easy

Author: leoluk

First Blood: flexerilla

After compromising the left-pad NPM package by guessing the author's NPM credentials (which happened to be the name of his cat, Lucy), you ended up with a shell somewhere deep inside a random company's continuous integration infrastructure.

Your goal is to escalate your privileges through this multi-stage challenge and pivot through the company network. Each stage of the challenge has its own flag - this is part 1.

See more details on the dedicated challenge page:

https://devops.allesctf.net/

Your session is stateful. Please share it with your team members - we have limited capacities. Terminate it unless you're currently working on it.

The flag format is different for this challenge.

Enterprise DevOps 2

Category: Systems / Network

Difficulty: Easier than you think

Author: leoluk

Dependencies: Enterprise DevOps 1

First Blood: RPISEC RPISEC

See more details on the dedicated challenge page:

https://devops.allesctf.net/

Your session is stateful. Please share it with your team members - we have limited capacities. Terminate it unless you're currently working on it.

The flag format is different for this challenge.

Hint: This is network-related. No need to nmap, all hosts are in /etc/hosts

Hint 2: Just because you can't do anything interesting, that doesn't mean nobody else in the network can.

Enterprise DevOps 3

Category: Systems / Network

Difficulty: Hard

Author: leoluk

Dependencies: Enterprise DevOps 1, Enterprise DevOps 2

First Blood: RedGKFRocket

See more details on the dedicated challenge page:

https://devops.allesctf.net/

Your session is stateful. Please share it with your team members - we have limited capacities. Terminate it unless you're currently working on it.

The flag format is different for this challenge.

Web========

kuchenblech1

Category: Web

Difficulty: Easy (but guessy)

Author: localo & A2nkF

First Blood: dcua

This Challenge can only be solved by the chosen one. While many have tried, no one has ever managed to solve it. Think you can do it? Then go ahead. But be warned, all your skills are going to be put to the test...

hax.allesctf.net:5555

Hint 1: Cookies are a very esoteric concept!

Hint 2: We agree, this challenge comes straight out of the eighth circle of hell

pdfcreator

Category: Web

Difficulty: Medium

Author: 0x4d5a

First Blood: dcua

A pdf conversion service. What could go wrong?

hax.allesctf.net:3333

code.zip https://static.allesctf.net/code-6c8fe52c26dec8c08d407bef5a52598d39dbf8b3.zip