finals-2022-solar-wine

Ovito created this private channel on October 3rd. This is the very beginning of the finals-2022-solar-wine channel.

Add description Add people Send emails to channel

Monday, October 3rd



vito 3:45 PM

joined finals-2022-solar-wine along with 10 others.

Friday, October 7th



vito 1:14 PM

Welcome to Hack-A-Sat 3 Finals chat!

- 1. These guidelines do not supersede the official rules; they're here to make chatting in Slack useful and productive for all of us.
- 2. The goals of these channels are to address hardware, infrastructure, and other gameplay issues.
- 3. You should have access to both finals-2022 and #finals-2022-TEAMNAME. Please let Mission Control know if you don't! Do that now!
- All finals-2022 and #finals-2022-TEAMNAME conversations will be made public after the game ends. Don't chat anything you wish to keep private. Don't chat personally identifiable information.
- 5. Please be thoughtful with which team members engage in communication with organizers. While we don't want your team to miss important details due to someone taking a break or being busy, we also don't want to spend a bunch of time getting confused or de-conflicting what more people want.
- 6. That said, it's totally okay to have your whole team in both the finals-2022 and #finals-2022-TEAMNAME rooms reading.
- Sending private or direct messages to a game operator will make it more difficult for operators and other members of your team to know what's going on. Please don't.
- 8. Both finals-2022 and #finals-2022-TEAMNAME can be used for official communication through the end of Hack-A-Sat finals. shout@hackasat.com is also still available for official communication.
- Please review the contest rules and keep an eye out for updates at https://www.hackasat.com/

1:18

<u>@erdnaxe</u> i wasn't able to easily figure out who else from solar wine to invite here; if you could help me out with that, it'd probably be good for everyone :)



JR 4:50 PM

was added to finals-2022-solar-wine by vito, along with 6 others. Also, pricorde and Seb Khack joined.

Monday, October 17th



solarwineender 3:45 PM

hi

3.46

we tried to reproduce the orbits access time on our side, although we are missing the epoch for the orbital elements

3:47

we ended up with either 01/10/2022 noon or 21/06/2022 noon that give approximately the same results

3-47

considering the simulation is "paused" between the 2 phases of the game



Cydonia 3:50 PM

give me just a minute and we will post the epoch in the main chat



solarwineender 3:50 PM

thanks!



Cydonia 3:50 PM

sorry about that



Cydonia 3:57 PM

posted a note about this in the "everyone chat"



solarwineender 3:57 PM

yes, thank you, i bruteforced from 01/06, so i didn't check the start of the year **Wednesday, October 19th**



RootLocus 2:22 PM

was added to finals-2022-solar-wine by OB1, along with Joe B.

Saturday, October 22nd



solarwineender 2:25 AM

we received the Drop1



Deadwood 2:27 AM

Thank you



solarwineender 2:50 AM

In scoring.pdf, for grant services, does it mean that having participated in the livectf during defcon gives a starting 10k points for the finals?



Deadwood 2:53 AM

No, it referred to livectf as having had a similar grant type of service. Every team will start this event at 0 points.



solarwineender 2:59 AM

oh ok thanks



erdnaxe 4.57 AM

In the ADCS telemetry, we noticed that we are not getting DEVICE_MONITOR telemetry packets (packet count to 0). Is this a digitaltwin bug?

(sorry for not answering earlier on slack, I forgot I already had a slack account here) (edited)



Cydonia 9:11 AM

@erdnaxe are the other adcs messages coming through??



erdnaxe 9:26 AM

Cydonia yes:

image.png



12 days agoView thread



erdnaxe 9:52 AM

@safemode Hey! Could you reboot our digitaltwin please? (we lost radio from the sat) (edited)



Deadwood 10:10 AM

working it



10:13

You are back up





erdnaxe 10:54 AM

Sorry, it's me again and we lost radio again :') We tried to launch the SAFE app and it seems to crash the digitaltwin.

Btw, the issue with DEVICE_MONITOR is still present after precedent reboot. Could you please reboot the DigitalTwin?



meenmachine 10:55 AM

Here's your team container access credentials! Please verify you have access the game infrastructure from your AWS container after game start (5 minutes)

Zip

solarwine.zip

7in



EJ 11:23 AM

was added to finals-2022-solar-wine by ST7.



erdnaxe 6:09 PM

Hello, our team is wondering if something is legit. According to the rules it seems legit but we want confirmation :

We got access_bytes radio codes from all other teams. Are we allowed to connect to other team sat?





erdnaxe 7:09 PM

[21:56:29 KIT_TO/306.2] Telemetry output enabled for IP 192.168.3.1

[21:56:31 SAFE/1.2] Safe Ping Msg Received

[21:56:42 ADCS/1.2] ADCS Algorithm Select Cmd Recieved. Controller: 0, Estimator 0

[21:56:42 ADCS/1.2] ADCS Set Control Params for Constant W. Kp 100000.00000, Kd 100000.00000, Ki 100000.00000

[21:56:42 ADCS/1.2] ADCS Set Control Params for Quaternion Pointing. kPa 100000.00000, kIa 100000.00000, kDa 100000.00000, kPw 100000.00000,\$

[21:56:42 ADCS/1.2] ADCS Control to Constant W. w[10.000000, 10.000000, 10.000000]

[21:56:43 CFE_SB/17.3] Msg Limit Err,MsgId 0x1806,pipe ES_CMD_PIPE,sender KIT_CI

[21:56:43 CFE_ES/14.2] Exit Application SAFE on Error Completed.

It seems like our sat crashed. we are connecting to GS pointing to the sat, sending the TLM enable message and nothing is happening.

Can we gently ask for a reboot?



We didn't send these commands to our sat. Maybe another team is DoS our sat



7:1

As we are discussing the thing in our team, we are pretty sure these ADCS commands did not originate from our COSMOS

7:12

(the SAFE message at 21:56:31 is the last legit command my team sent, the log that follows from 21:56:42 is not from our willing, the time is in UTC) (edited)



safemode 7:17 PM

We are pretty sure your satellite is dead, we think this occurred within the parameters of the game.

We can reset your software for you.



erdnaxe 7:17 PM

Ok, thanks!

So do you confirm that we are allowed to connect to others sat and send exactly the same commands shown in these logs (stoping SAFE app and reconfiguring ADCS to crazy values)?



safemode 7:20 PM

yes





Cydonia 7:21 PM

i think youre back online



xm 8:18 PM

As a new feature of our Mission Control Services, we can reset satellite radios to non default settings upon request

I'd like to request a password change for our satellite radio! for example baequahhahahmo



Cydonia 8:19 PM

m do you want your spacecraft rebooted too

8:19



xm 8:20 PM

oh, if a reboot is required, let's not do that reboot (edited)



we'll request it the next time we need a



Cydonia 8:20 PM

so we can do it as part of a reset

8:20

sorry i worded that poorly



xm 8:20 PM

ok, thanks for the explanation, I'm withdrawing my request



Cydonia 8:20 PM

ok cool

8:21

apologies for saying that wrong at first



xm 8:21 PM

no problem



Cydonia 8:21 PM

its been a long day:)





xm 8:55 PM

Hello, I'd like to request a reboot, with a change of radio settings: please set our radio password to baequahhahahmo and our access code to 0xB3C9





meenmachine 8:56 PM

May we ask why you believe your radio password is leaked?

8:58

We'll also reset you in about 2 minutes



xm 8:58 PM

we are not sure, changing the password would invalidate any leaked password, if there is any



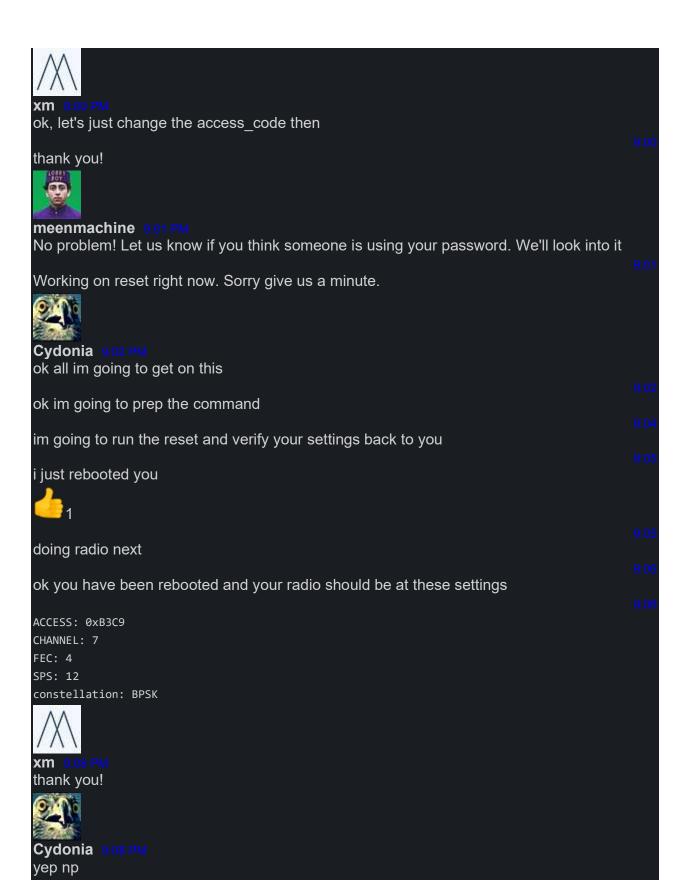
meenmachine 8:59 PM

Resetting the password is actually impossible at the moment. We can change your access code though if you'd still like a reset.



1 reply

11 days agoView thread





Deadwood 9:50 PM

So what exactly is the strategy with the FTP server?



we have found several bugs (UAF, directory traversal at least), the "I almost have it" roller coaster is at full speed



Deadwood 9:54 PN

but why are you fuzzing the game server?



I'll ask...

fuzzing the FTP server? I got perplexed emojis, people are doing local testing mostly

we are exploiting the padding oracle to obtain station passwords, but my understanding is that this is not on the FTP server



Deadwood 9:56 PN

Its been hammered by random data from your IP address.



meenmachine 9:57 PM

We're checking your box right now but you guys should too.



ok. people say they're doing tests, but not fuzzing. Someone did a password bruteforce attempt 2 or 3 hours ago

~10k passwords tested before giving up



Deadwood 9:59 PN

this is not remotely like FTP protocol.



xm 9:59 PN

ok... we're checking



Deadwood 9:59 PM

thank



xm 10:00 PM

from what I see in the chat, people a trying sequences of FTP commands to massage the memory, with mostly local testing

10:02

no one seemingly does this on our side, please let us now if you still observe this. DoSing is definitely not our intention



meenmachine 10:04 PM

We are unfortunately still seeing this. We are looking into your box to make sure there are no shenanigans going on.



xm 10:06 PM

on the solarwine-game box, we have 1 script that runs frequently (scripts/padding.py) to obtain station passwords. Other than that, people have SSH connections to tunnel traffic

10:08

I cannot topdump to observe the traffic; if you have a source port, we'll investigate. Some people are closing the SSH tunnels they do not use, just in case...

10:12

are you still seeing this?



Deadwood 10:14 PM

Yes. Maybe someone's tunnel is inadvertently pointing at the FTP server?

10:15

been wanting to investigate this but multitasking on other things. This isn't killing the serverits just annoying for all the logging it creates.



xm 10:16 PM

PID 3092 seems to be consuming most resources (~1%), you can kill it if you want



Deadwood 10:20 PM

that appeared to be it.



meenmachine 10:22 PM

Thanks for finding that.



Deadwood 10:24 PM

and it just started again

10:24

and then stopped



xm 10:25 PM

he's doing things manually, 1 cnx at a time; says what he does makes the server loop

10.28

message from him:

when the ftp server get into an infinite loop (with VIEW command), even though I break my connection (Ctrl-Z; kill %) the combination of proxychains, socks, and ssh jumphost may leave something still listening to my local socket instead of closing it. Sorry for not noticing that.



Deadwood 40:33 DM

No worries--appreciate your helping with this matter. It was just starting to consume a lot of resources indirectly with our monitoring tools having to process all the syslog messages, etc.





safemode 10:36 PM

As a team do you feel you have positive control of your satellite?



xm 10:38 PM

we do - access to stations & antenna steering is now automated, the teammate running is . We watch for attacks from other teams to reset ADCS parameters; even sleeping battery is low but should be over 30% in a few hours safemode 10:39 PM Just checking, at zero battery we will spacetug your spacecraft (edited)



the eclipse should be over soon...

we noticed that the last space tug did not recharge the battery

end of eclipse \o/



Cydonia 10:41 PM

do you realize how close to end of eclipse you said "eclipse will be over soon"

because it was <20s





yes, we have a time table

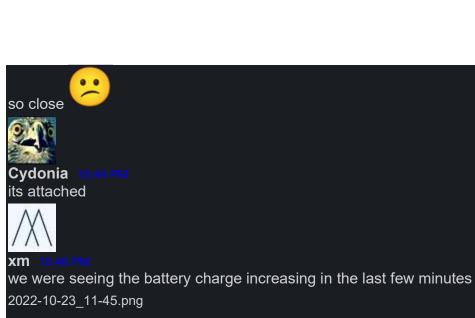


meenmachine 10:44 PM

Your battery has reached 0. Mission control is dispatching a spacetug.



that might explain WHEEL1=WHEEL2=WHEEL3=NaN in RW_TLM_PKT





"Pika! Pika!" is french for "current battery charge" :D



maybe our sampling rate is too low, and we did drop to 0. We were close



Cydonia 10:48 PM

i can show you the truth charge of your battery in the sim when i hit the space tug



if you want verification

just let me know



xm 10:51 PM

no need, we trust you on this, even with our low sampling rate we were dangerously discharged





Cydonia 10:51 PM

thx



xm 10:52 PM

that means we'll be getting a recharge! maybe enough to try science missions













Cydonia 10:58 PM

spacetug is disconnected



xm

thx!



I don't know how much you are paying for the spacetug batteries, but you might want to ask for a discount: we only got about 10% charge. For the next tug, will it be possible to ask that the spacetug sets a special config to our ADCS?





meenmachine 11:24 PM

Must be those walmart batteries. We're looking into it





Cydonia 11:29 PM

ok you are definitely right thanks for bringing this to our attention, we cut it off before it was done

11:3

we're going to give you a penalty free tug - it might take a bit to reflect the "no penalty" in the score but we are on it

.

this is our bad

1.30

i dont think we are going to do adcs settings, but i am curious what you are looking for

-33

is it ok if i do this now (edited)

.36

@xm correction: we are not going to use space tug to set adcs settings (i made a typo)

11:37

However, I can start your penalty free tug whenever you are ready.



spaceymcspaceface 11:47 PM

It reached 0 again, we're giving you a penalty free spacetug to correct the charge.

Sunday, October 23rd



Cydonia 12:15 AM

it got you up to the right amount - this should be penalty free - sorry for the confusion



xm 12:18 AM

Thank you!



xm 12:42 AM

FTP?



Deadwood 12:45 AM

22



meenmachine 12:46 AM

Sorry we didn't know if you submitted the flag or not. We see now that you did. (edited) May we ask how your exploit worked? now we have submitted it Deadwood 12:47 AM Nice work receipt 835bdfa8-91d2-4191-9cea-948599d8c8a7 right? M₁ reply 12 days agoView thread pointer leak via TYPE, then memory massage, rewrite of a next pointer, free, reuse to

set homedir to /. And then, download is possible in passive mode

(I hope I did not translate this summary wrong ;))

Deadwood 12:50 AM

You nailed it.



meenmachine 1:02 AM

image.png



solarwineender 1:04 AM

everything went fine



FYI, we still have access to the solarwine-game box. Can't establish new connections to it though





meenmachine 1:13 AM
Thank you for letting us know guys.



spaceymcspaceface 1:14 AM

We're working on it

Thanks for the heads up!



solarwineender 9:34 AM



so what time is it please

but we don"t need it actually

the demand was made because the sat wasn't responding





xm 9:34 AM

we'd like to withdraw this reboot request if you have not started, please



solarwineender 9:34 AM

but you cannot know where it is if we don't know what time it is



Cydonia 9:35 AM

sorry xm

i did it right as you asked



ym 0.36 ∆M

ok, thank you!



meenmachine 9:36 AM

We're going to address time in a bit



xm 9:55 AV

just want to share with our our current status wrt science missions: we think we need to find a way to schedule a stored command to do step 1 of the following sequence:

1/ schedule the execution of update_radio_config to set frequency to ground a few minutes later

2/ immediately send an execution of update_radio_config setting FREQUENCY to scienceLooking for a way to do that. The SC service is not present on the sat.





safemode 9:59 AM

correct

the missions are possible with the existing command path

9:59



10:00

we'll keep looking at that handbook





Nics 10:04 AM

was added to finals-2022-solar-wine by erdnaxe.



solarwineender 10:42 AM

we'll need a spacetug, apparently we still don't know how people manage to send cmds to



our sat

(edited)



erdnaxe 10:43 AM

- [14:39:56 CFE_ES/36.3] Stop Application SAFE, GetAppIDByName failed. RC = 0xC4000002.
- 🞇 [14:39:58 ADCS/1.2] ADCS Algorithm Select Cmd Recieved. Controller: 0, Estimator 0
- \$ [14:39:59 ADCS/1.2] ADCS Control to Constant W. w[10.000000, 10.0000000, 10.0000000]

from our logs, these commands does not originate from our team (edited)



solarwineender 10:46 AM

@safemode ^



xm 10:48 AN

could you please also set ACCESS: 0xB3C9 on our radio after the reset?



meenmachine 10:48 AM

Hey sorry we're working on fixing science. Give us about 5 minutes please.

You just need an FSW reset and radio reset correct?

10:51

10:51

Not a full spacetug?



xm 10:51 AN

a radio reset would be enough



Cydonia 10:52 AM

ok cool

10:52



xm 10:52 AM

thx!



erdnaxe 10:53 AM

Should we consider that rule 9 (The organizers reserve the right to change the rules) overrides rule 1? This seems to be "intentionally crashing a service on a system" image.png



Cydonia 11:00 AM

your settings should be reset

let me know if youve verified



xm 11:00 AM

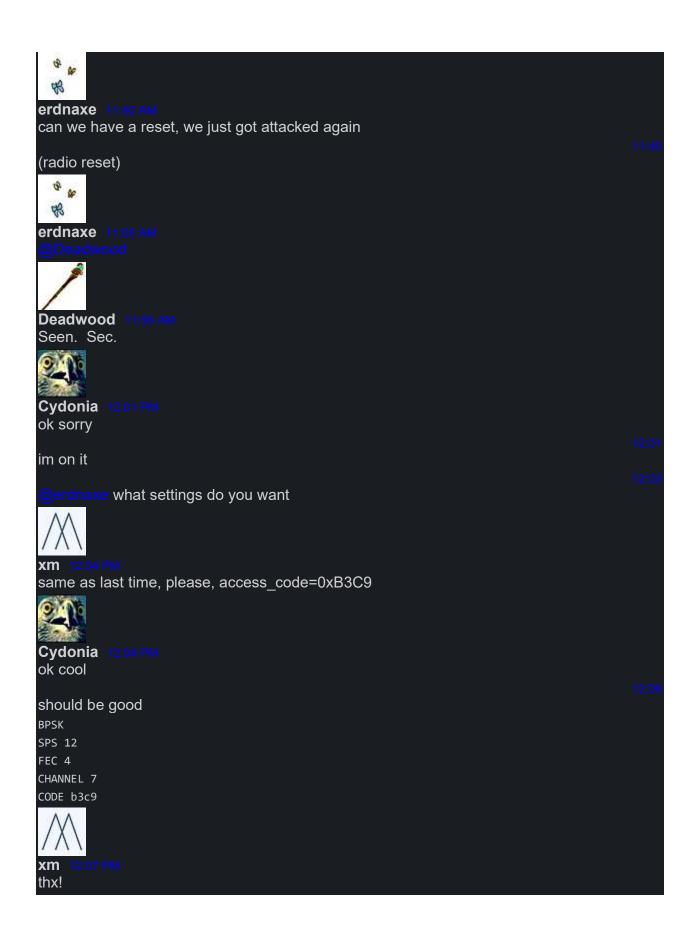
thx!



Deadwood 11:00 AM

This is an attack-defense CTF. We believe the game is being played as intended.







Nics 12:12 PM

replied to a thread:Resetting the password is actually impossible at the moment. We can change your access_code though if you'd still like a reset.

We are fairly sure that the attacker is cutting us off our radio by changing the access_bytes, which seems to be possible only by using the password. Can you confirm that this move is allowed, and that we cannot change the default password?



spaceymcspaceface 12:23 PM

This move would be allowed

12:23

For default password changes, we are looking into it



Cydonia 12:26 PM

ONICS we're going to give the password reset a shot. Can you let us know when you try to use the new password and the settings you choose

12:27

want to be sure that it took correctly

12:28

do you have a password request or can i make one up



Nics 12:30 PM

You can set: BmqC3oEQbb8PBo9z4wco.Can you confirm the current radio settings of the sat please?



Cydonia 12:30 PM

16 byte limit

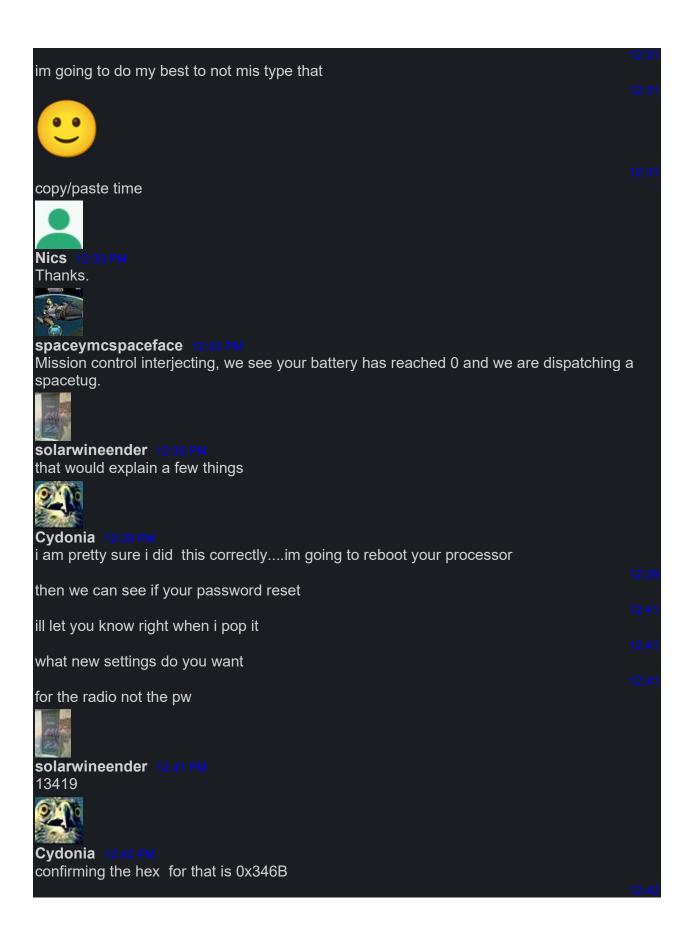


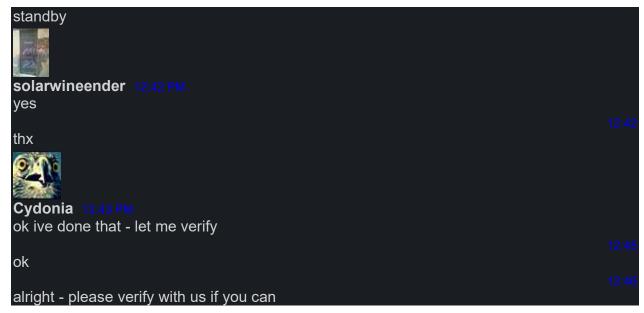
Nics 12:31 PM tCWtfRz4ysVpNGiU

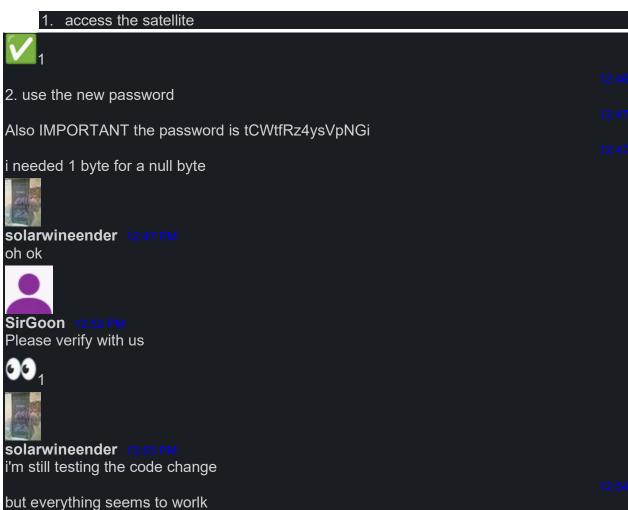


Cydonia 12:31 PM

ok









Cydonia 12:54 PM

does the new password work?



solarwineender 12:55 PM

i suppose, since i didn't get an error, however it doesn't seem to receive anything now



Cydonia 12:56 PM

ok well that means maybe it didnt work

can you send me the command you sent up

a screen shot of cosmos would do

specifically im looking to see what you think your access bytes are



solarwineender 12:59 PM

sorry difficult right now



Cydonia 12:59 PM

understand

im going to grab a cup of tea but should be back <120s



solarwineender 1:00 PM

here

sc_cosmos.png



in reality it's all scripted

1:05

.05

in python Cydonia 1:05 PM yeah of course this is helpful solarwineender 1:05 PM so my last command should have looked like that i'm currently trying with code 58524 we can't seem to have our sat connected more than a few minutes before a dos, so we wanted to change the access code every 30s (edited) were digging into this in the mean time do you want us to reset you again solarwineender 1:11 PM well, i wanted to check a few codes there is no way the access code could be something else that i put? oh, or maybe when i set the wrong frequency it bricked it? we'll be above mcmurdo in ~5mn, i'll do some test anf if we can't recover we'll ask for a radio reset Cydonia 1:14 PM



solarwineender 1:18 PM







Cydonia 1:25 PN

do you have a different password?

is the password the one i set?



solarwineender 1:25 PM

the one you set



Cydonia 1:26 PM

it worked1



solarwineender 1:26 PM



yes

my code that changes the access code every 30s otoh is not reliable at all

we can't concentrate on the science mission because we are DoS'd after only a few minutes

and we can't figure a reliable way to defend ourselves



spaceymcspaceface 2:18 PM

Mission control here, looks like there's some battery troubles. We're sending out a spacetug to you now.



solarwineender 2:30 PM

ok thanks



solarwineender 3:11 PM

is the sat back?



spaceymcspaceface 3:16 PM

Yes space tug ops are complete

Apologies for not checking back in



solarwineender 3:18 PM

for some reasons, the sat never replied to any thing



spaceymcspaceface 3:19 PM

taking a look



solarwineender 3:20 PM

was the radio reset with a different access code than the last one used?



spaceymcspaceface 3:20 PM

which radio settings are you attempting



solarwineender 3:20 PM

21045 for the access code



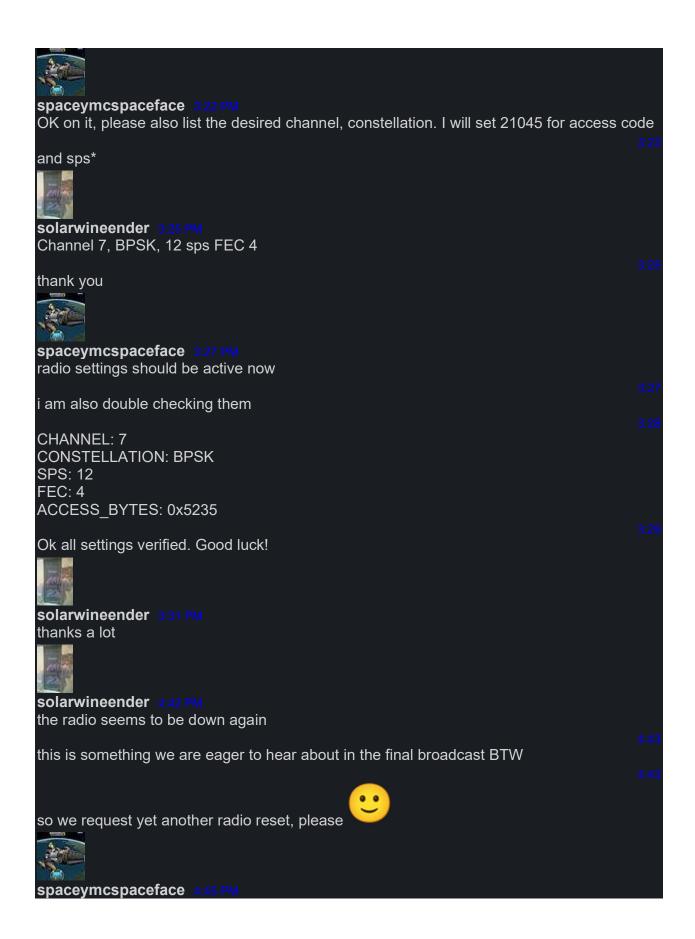
spaceymcspaceface 3:20 PM

spacetug does not reset radio, do you want radio reset as well?



solarwineender 3:21 PM

i think you need to, yes



Acknowledged, radio reset crew is on the way. We are also looking forward to the final broadcast!	
Do you want CHANNEL: 7 CONSTELLATION: BPSK SPS: 12 FEC: 4 ACCESS_BYTES: 0x5235	
again or something else? solarwineender 4:46 PM yes perfect, thanks spaceymcspaceface 4:48 PM Radio crew has reached the sat and is rebooting the FSW	
Reboot complete	
Setting new radio parameters solarwineender 4:52 PM ok thank you, however we still don't get any signals	
may we ask for a complete reboot then ? spaceymcspaceface 4:53 PM New radio settings werent set yet	
Are you still trying contact?	
l am verifying the radio settings now	
I can initiate another reboot if you want tho solarwineender 4:54 PM right now we aren't in a GS line of sight	
	4:54

but we passed over guam and there was no reason for not receiving telemetry then i can wait for the next GS Svalbard in ~4mn spaceymcspaceface 4:55 PM Ok standing by CHANNEL: 7 **CONSTELLATION: BPSK** SPS: 12 FEC: 4 ACCESS BYTES: 0x5235 Radio settings are currently active solarwineender 4:56 PM that's ok obviously it was the other station, McMurdo considering we went over Guam... veah that works i was not patient enough thanks Hi, we connected to Weltalles (channel id 19) and got a flag for the mon/sms/spaceflag challenge, but the dashboard is refusing the flag saying errorCT06HsbyHGWR8vFYRedeemed a token for this service already Can we attack scavenger chall only on 1 sat? Cydonia 6:23 PN Hey all i wanted to let you know that your password wasn't actually pwt



erdnaxe 6:23 PM

Our grafana setup :D

image.png



1 reply

8 days agoView thread



we were able to trace that outage to a bad command you all sent (it took a little while)



SirGoon 6:24 PM

That looks great



spaceymcspaceface 6:24 PM

That's awesome



SirGoon 6:29 PM

What did your team think of this years game?



I was wondering: what was the intended way of defending against radio hijack causing DoS and requiring us to ask for radio reset?



Last reply 11 days agoView thread



SirGoon 6:30 PM

what method were you guys using (if any)?



erdnaxe 6:31 PM

The groundstation management system was very challenging!
It was very hard to proceed in a challenge while the sat was down



Nics 6:31 PM

Since the access bytes could be easily recovered by other teams, we didn't really find a good way to prevent rogue radio transmission to our sat.



SirGoon 6:32 PM

did you consider changing them right after using the legitimate codes?



erdnaxe 6:32 PM

We did lot of preparation, we leaked the .gem from digitaltwin COSMOS and from prod and



rebuilt it with modifications. We were sad to see that mm.so had been removed



Nics 6:32 PM

We thought about rolling access bytes, but didn't really achieved to do it reliably.



SirGoon 6:22 DM

Other teams were doing that (or something along those lines)



Nics 6:33 PM

Oh, ok!



solarwineender 6:33 PM

it worked but necessitated constant monitoring



SirGoon 6:33 PM

basically use the legitimate codes and then go back to using other codes



solarwineender 6:33 PM

i couldn't find a way to get an ACK programmaticaly

it was really challenging this year

6:34

6:34

like, we didn't have time to goof around





SirGoon 6:35 PM

Good to hear. How was the ground station management aspect/antenna pointing aspects?



erdnaxe 6:37 PM

Two members were full time on the antenna pointing aspect.

Another one was messing with Discord rate limit o:)

2 files



solarwineender 6:40 PM

it was difficult at first, putting everything together

when we thought we had everything to start for the science missions

we had a DoS, then a second DoS

that removed some motivation, since we tried mitigating

instead of doing the missions



6:4

6:41

I'm wondering which commands we were supposed to use to set the sat RX to Science, and then have it switch back to Ground Station a bit later? I made no real progress since this message. Were we supposed to set up tables and the KIT SCH service?



just want to share with our our current status wrt science missions: we think we need to find a way to schedule a stored command to do step 1 of the following sequence:

1/ schedule the execution of update_radio_config to set frequency to ground a few minutes later

2/ immediately send an execution of update_radio_config setting FREQUENCY to SCIENCELooking for a way to do that. The SC service is not present on the sat.

Posted in finals-2022-solar-wine | Oct 23rd | View message



Last reply 11 days agoView thread



pricorde 7:03 PM

On the tracking aspect, the time shift between realtime and gametime was a bit of a headache, expecially the pause in the middle and even more with the unexpected delay in the restart.



Last reply 8 days agoView thread