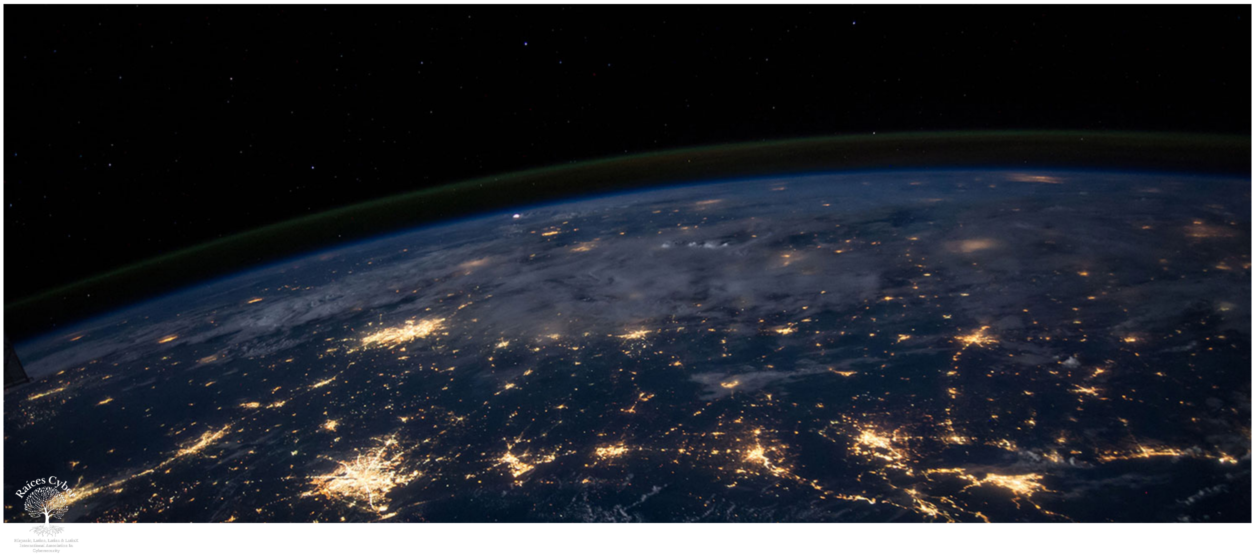
Raices Cyber
Hispanic, Latino, Latina & LatinX International Association In Cybersecurity

Cyber Apocalypse 2024

by HTB

https://www.hackthebox.com/events/cyber-apocalypse-2024

https://ctf.hackthebox.com/event/details/cyber-apocalypse-2024-hacker-royale-1386

Team Name: Raíces Cyber

About

Official team of Raíces Cyber for this event.

Respect and kindness are our golden rules.

Let's build a positive and supportive team environment together.

Members

1. @Davi Torres (member of Toronto Chapter)
2. @Lourdes
3. LeonVQZ
4. hackerdemic
5. KaliBlue
6. Luigiguti01
7. Makanaki
8. 0dysseusz
9. @Zel
10. shortstickofdynamite
11. @Leonardo Gutierrez
12. @Cherry

Tracking Board

Please add your name to the challenge you are working on.

Misc

#	Challenge Name	Currently Working	Solver + Flag
1	Colored Squares		
2	Were Pickle Phreaks		
3	Cubicle Riddle		
4	Unbreakable		@Davi Torres HTB{3v4l_0r_3vuln??}
5	Path of Survival		
6	Stop Drop and Roll		@Davi Torres HTB{1_wiLl_sT0p_dR0p_4nD_r0Ll_mY_w4Y_oUt!}
7	MultiDigilingual		
8	Were Pickle Phreaks Revenge		
9	Quantum Conundrum		
10	Character		@Davi Torres HTB{tH15_1s_4_r3aLly_l0nG_fL4g_i_h0p3_f0r_y0Ur_s4k3_tH4t_y0U_sCr

#	Challenge Name	Currently Working	Solver + Flag

Comments: (anything!)

Forensics

#	Challenge Name	Currently Working	Solver + Flag	Notes / Tips / Clues
1	Fake Boost	@Leonardo Gutierrez	1/2 `HTB{fr33_N17r0G3n_3xp053d!_` 2/2	1/2 Packet 328 has a payload that when converted from Hexdump outputs PowerShell commands. 2/2 There is an encryption function that might be vulnerable to AES-CBC Padding Attack.
2	Phreaky		@Davi Torres HTB{Th3Phr3aksReadyT0Att4ck}	Extract 15 emails from the `.pcap` then extract all zip attachments and decompress with the passwords from the body of each email. Then combine all parts in a single PDF file.
3	Oblique Final			
4	Urgent		@Angel Ojeda HTB{4n0th3r_d4y_4n0th3r_ph1shi1ng_4tt3mpT}	base64 decode, then URL Decode to get the plain text email.
5	Confinement			

#	Challenge Name	Currently Working	Solver + Flag	Notes / Tips / Clues
6	Game Invitation			
7	Data Siege		1/3 flag 2/3 flag `Very_S3cr3t_S` 3/3 flag `0r3d_1n_7h3_h34dqu4r73r5}`	1/3 2/3 from `strings` command on `aQ4caz.exe` (port 8000). 3/3 from a PowerShell in packed 119 (port 1234).
8	Pursue The Tracks		@Leonardo Gutierrez HTB{p4rs1ng_mft_1s_v3ry_1mp0rt4nt_s0m3t1m3s}	Use Zimmerman tools MFTECmd to parse $MFT file using the tool
9	An unusual sighting		@Davi Torres HTB{B3sT_0f_luck_1n_th3_Fr4y!!}	Read the logs to answer the questions.
10	It Has Begun		@Davi Torres HTB{w1ll_y0u_St4nd_y0uR_Gr0uNd!!}	The key is partially in the comment of the SSH public key and partially in base64 in the crontab line.

Comments: (anything!)

Web

#	Challenge Name	Currently Working	Solver + Flag	Notes / Tips / Clue
1	TimeKORP		@Davi Torres HTB{t1m3_f0r_th3_ult1m4t3_pwn4g3}	Code execution with
2	KORP Terminal		@Davi Torres HTB{t3rm1n4l_cr4ck1ng_sh3n4nig4n5}	`username` is vulnera And the password I
3	Flag Command		@Angel Ojeda HTB{D3v3l0p3r_t00l5_4r3_b35t_wh4t_y0u_Th1nk??!}	check POST request commands.
4	Apexsurvive			
5	Percetron			
6	SerialFlow			Vulnerable to Templ `uicolor=red`
7	LockTalk		@Davi Torres HTB{h4Pr0Xy_n3v3r_D1s@pp01n4s}	TO get a token, nav `http://IP:PORT//ap use this to forge t https://github.com/ 39227
8	Testimonial			
9	Labyrinth Linguist		@Davi Torres HTB{f13ry_t3mpl4t35_fr0m_th3_d3pth5!!}	It is vulnerable to Exploited with STTI (https://github.com

Comments: (anything!)

Reversing

#	Challenge Name	Currently Working	Solver + Flag	Notes / Tips / Clues
1	Crushing			
2	MazeOfPower			
3	FlecksOfGold			
4	Metagaming			
5	QuickScan			
6	FollowThePath			
7	LootStash		@Davi Torres HTB{n33dl3_1n_a_l00t_stack}	Use the commands `strings`
8	PackedAway			
9	BoxCutter		@Davi Torres HTB{tr4c1ng_th3_c4ll5}	Use `ltrace`

Comments: (anything!)

Crypto

#	Challenge Name	Currently Working	Solver + Flag
1	Dynastic		@Angel Ojeda HTB{DID_YOU_KNOW_ABOUT_THE_TRITHEMIUS_CIPHER?!_IT_IS_SIMILAR_TO_CAES
2	Makeshift		@Angel Ojeda HTB{4_b3tTeR_w3apOn_i5_n3edeD!?!}
3	ROT128		
4	Tsayaki		
5	Permuted		
6	Partial Tenacity		
7	Arranged		
8	Blunt		@Cherry HTB{y0u_n3ed_a_b1gGeR_w3ap0n!!}
9	Iced TEA		
10	Primary Knowledge		@Cherry HTB{0h_d4mn_4ny7h1ng_r41s3d_t0_0_1s_1!!!}

Comments: (anything!)

Pwn

#	Challenge Name	Currently Working	Solver + Flag	Notes / Tips / Clues
1	Gloater			
2	Maze of Mist			
3	Oracle			
4	Sound of Silence			
5	Deathnote			
6	Rocket Blaster XXX			There is a buffer overflow at the 41st character. I crafted I payload that jumps to function `fill_ammo` and also overflows all three parameters but it fails at the `printf` right before printing the flag.
7	Pet Companion			
8	Writing on the Wall		@Davi Torres HTB{3v3ryth1ng_15_r34d4bl3}	There is a buffer overflow and can be exploited by crafting a payload to overwrite the values being compared and return a match.
9	Delulu			I think that by disassembling you can get the ID number. No success brute-forcing so far…
10	Tutorial		@Davi Torres HTB{gg_3z_th4nk5_f0r_th3_tut0r14l}	Theory plus math.

Comments: (anything!)

Blockchain

#	Challenge Name	Currently Working	Solver + Flag	Notes / Tips / Clues
1	Ledger Heist			
2	Lucky Faucet			
3	Recovery			
4	Russian Roulette			

Comments: (anything!)

Hardware

#	Challenge Name	Currently Working	Solver + Flag	Notes / Tips / Clues
1	Flash-ing Logs			
2	The PROM			
3	Rids		@Davi Torres HTB{m3m02135_57023_53c2375_f02_3v32y0n3_70_533!@}	`echo -n '{"tool": "pyftdi", "cs_pin": "url": "ftdi://ftdi:2232h/1 "data_out": ["0x03"] "readlen": 53}' | nc <IP> <PORT>`
4	BunnyPass		@Davi Torres HTB{th3_hunt3d_b3c0m3s_th3_hunt3r}	Read the messages in the queue `factory_idle`.
5	Maze		@Davi Torres HTB{1n7323571n9_57uff_1n51d3_4_p21n732}	Look into the PDF

Comments: (anything!)