

Copyright © 2026 ROOTCON® Conference Inc. All rights reserved.

THE ROOM IS ALIVE BEFORE THE MIC IS.

Before anyone touches a microphone, ROOTCON is already in motion. Friends who have not seen each other since the last con resume conversations as if the year between them was only a brief outage. First-timers study the map, then follow the noise. Badges blink. Laptops open. Somebody is hunting for coffee, a cable, or the one person who knows why the demo worked last night and refuses to work now. The day rarely begins onstage. It begins with a small problem and three people leaning over it.

Goons catch small disasters before they become public ones. Village crews power up tables assembled from plans, borrowed gear, and stubbornness. A question passes between strangers and becomes a sketch, a command, a fix. There is no ceremony to it - just knowledge handed across the room while it is still warm. That current has carried ROOTCON through twenty editions. The venues change. The instinct remains: show up, share what works, and make room for whoever arrives next. This book begins inside that noise.



THE SIGNAL

SHOW UP.
SHARE WHAT WORKS.
MAKE ROOM.

That is how knowledge travels through ROOTCON.

THE TWENTIETH EDITION



This is a field record of the people who kept showing up. Speakers arrived willing to share unfinished thinking, including the parts that still made them nervous. Builders turned borrowed tables, tangled cables, and stubborn ideas into villages. Goons carried work most attendees never saw. People came with questions, broke things carefully, argued over better ways to put them back together, and left with collaborators they had not known that morning. The conference filled the schedule. The community filled everything around it.

Homecoming fits the rhythm of this twentieth edition. Familiar faces return with new scars, new tools, and better questions. First-timers walk into a room shaped by people they have never met, then begin changing it themselves. That exchange is the real continuity of ROOTCON: experience passed forward without being polished into mythology. What survives is practical, generous, and a little unruly. It lives in the hallway explanation, the late-night fix, and the invitation to pull up a chair.

THE RECORD

THE CONFERENCE FILLED THE SCHEDULE. THE COMMUNITY FILLED EVERYTHING AROUND IT.

Twenty editions, carried forward by the people in the room.

WELCOME HOME.

ROOTCON 20: Homecoming is deeply personal to me.

Twenty editions in, ROOTCON still refuses to be just an event. It has been our proving ground, our classroom, our playground, and, for more of us than we probably admit, a second home.

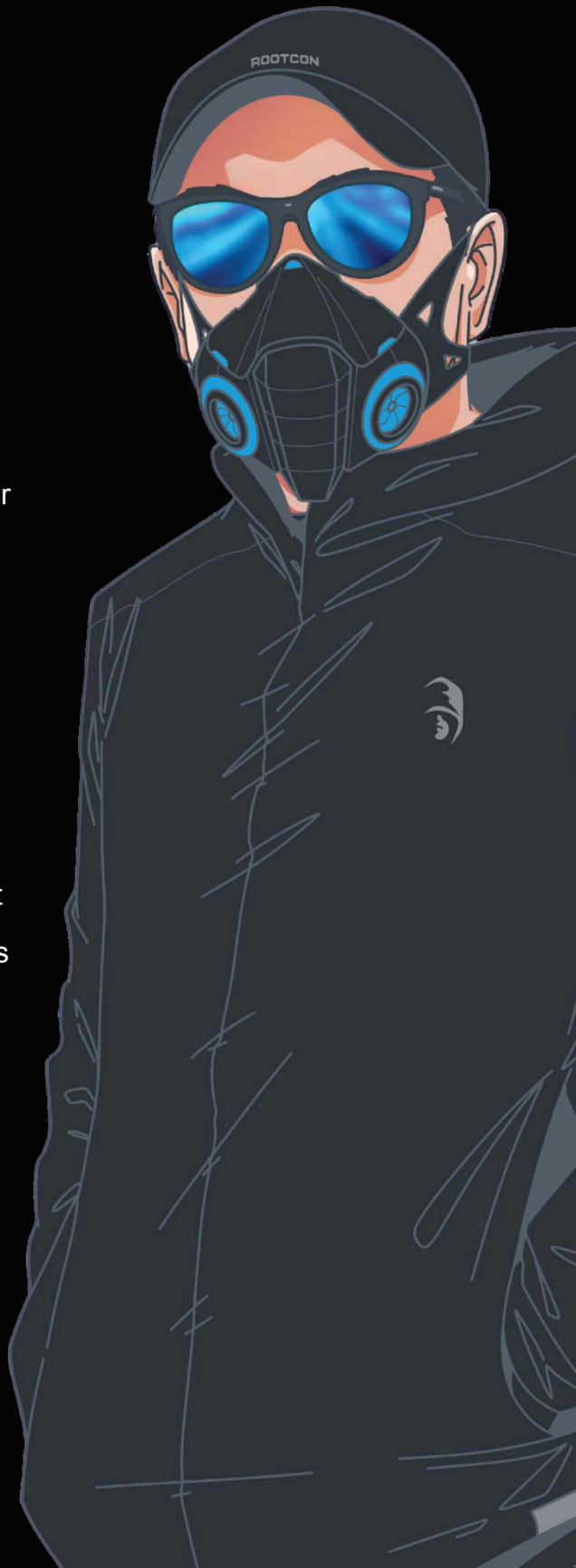
This community was built by people who kept showing up. They came to listen, then stayed to contribute. They stayed late at the villages to help a stranger finish a challenge. They shared tools without guarding the trick, passed on hard-earned lessons, welcomed newcomers into the circle, and kept the signal moving from one generation to the next.

Homecoming gives us a reason to look back, but nostalgia is not the assignment. We are here to return sharper, more generous, and more curious than before.

Anyone who has spent even one day inside ROOTCON already knows: the venue changes. The stage goes dark. The schedule gets folded into a bag and forgotten.

What remains is the people. Welcome home.

Semprix



CONTENTS

06 HOMECOMING

07 GOONS / DON'T POKE THE BEAR

08 THE CHRONICLE

16 PEOPLE, BADGES & OBJECTS

22 VILLAGES & COMMUNITIES

30 CONTESTS & EXPERIENCES

36 TALKS & SPEAKERS

50 KEYNOTE SPEAKERS

51 CFP REVIEW BOARD

52 PARTIES / ZERO-HOUR

54 MOVIE NIGHT

56 SPONSORS

60 ACKNOWLEDGMENTS

61 CLOSING / WORLD DOMINATION

WE FOUND OUR WAY BACK.

TWENTY EDITIONS LATER, HOMECOMING IS NOT ABOUT GOING BACK. IT IS ABOUT RECOGNIZING WHAT NEVER LEFT.

Homecoming is not a return to one building, one stage, or one version of ourselves. ROOTCON has changed rooms, plans, scale, and shape, but the current underneath it has remained stubbornly familiar: the noise before the doors open, a badge spotted across the hallway, and a conversation resumed without introduction.

People return carrying new tools, harder questions, and stories gathered between editions. Some come back as speakers, builders, village leads, Goons, mentors, or the person quietly holding a cable while somebody else fixes the problem. Others return because this remains one of the few rooms where curiosity is welcome even when it takes things apart.

That continuity is easy to miss because it rarely stands under a spotlight. It lives in borrowed chargers, hallway explanations, late fixes, shared meals, and the patient answer offered to someone asking a question for the first time.

First-timers arrive without the history, then become part of it before the weekend is over. Someone explains an unwritten rule. Someone slides over and makes room at the table. A stranger becomes a teammate, and by the time names are exchanged, the work has already started.

That is what comes home at the twentieth edition: not a perfect memory, but a living habit of showing up. The old stories matter because they taught us how to build the next room, invite the next voice, and pass forward what would otherwise disappear.

We are not rebuilding an old moment or trapping ROOTCON inside nostalgia. We are recognizing what endured, being honest about what changed, and choosing what deserves to travel with us. Homecoming is the pause before the next question, the breath before the room gets loud again, and the signal moving forward.

WE DID NOT COME BACK TO REPEAT THE PAST.
WE CAME BACK TO BUILD WHAT HAPPENS NEXT.

GOONS

ROOTCON is built by people with different skills who return each year to assemble the conference, keep it moving, and make room for everyone who walks through the doors. Their work turns plans, cables, tables, radios, and last-minute fixes into the experience the community recognizes as ROOTCON.

They carry the load before the doors open and stay until the last loose end is tied. Someone traces the dead cable, resets the room, and catches the small problem before it becomes everybody's problem.

The work asks for judgment, timing, patience, and a willingness to step in. Goons move between talks, villages, registration, and hallways, turning plans into an experience people can enter and remember.

They are part of the welcome, too. First-timers get directions, speakers get help, villages get another pair of hands, and tired teammates get covered without ceremony.

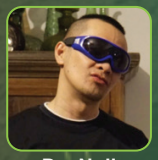
And the warning? DON'T POKE THE BEAR. It is less a threat than a field-tested operating principle. If a Goon has found thirty quiet seconds, approach with coffee, context, and a good reason. Poke without purpose and you may be handed the problem you interrupted.

ROOTCON happens because the Goons make it happen, from inside every moving part.


ApolByte


ar33zy


DeityJubilum


DevNull

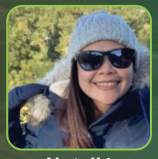

Eman0n


Encrypted84


Highta1l


Mogul


Napz


Nutell4


Schiaparelli


Sh33pdog


ShipCode


Tikbalang


TheJanitor


Whiskah


Whiteflower

DON'T POKE THE BEAR

THE SIGNAL KEPT MOVING.

DATES AND ROOMS GIVE THE STORY A SKELETON. THE PEOPLE WHO FILLED THEM GIVE IT A PULSE.

History rarely arrives in perfect order. It survives in old photographs, venue names, hallway conversations, and the people who remember which cable failed before the doors opened.

ROOTCON began with a date and a room, then refused to stay still. It changed cities, formats, and scale while holding onto one exchange: learn something difficult, then share it.

A timeline keeps count. The community gives it a pulse - through brave first talks, borrowed gear, improvised fixes, and questions carried into the next edition.



HANDURAW. ONE DAY. ROOTCON 1.







20 DECEMBER 2008 / HANDURAW PIZZA / CEBU CITY

On 20 December 2008, ROOTCON 1 gathered at Handuraw Pizza in Cebu City. The surviving picture is wonderfully spare: one day, one room, a stack of presentations, and people willing to start. Before long programs and multi-day schedules, curiosity was enough to make the room matter.

Early sessions set the tone: look closely at what systems reveal, understand the terrain before touching it, and leave with something practical enough to use.

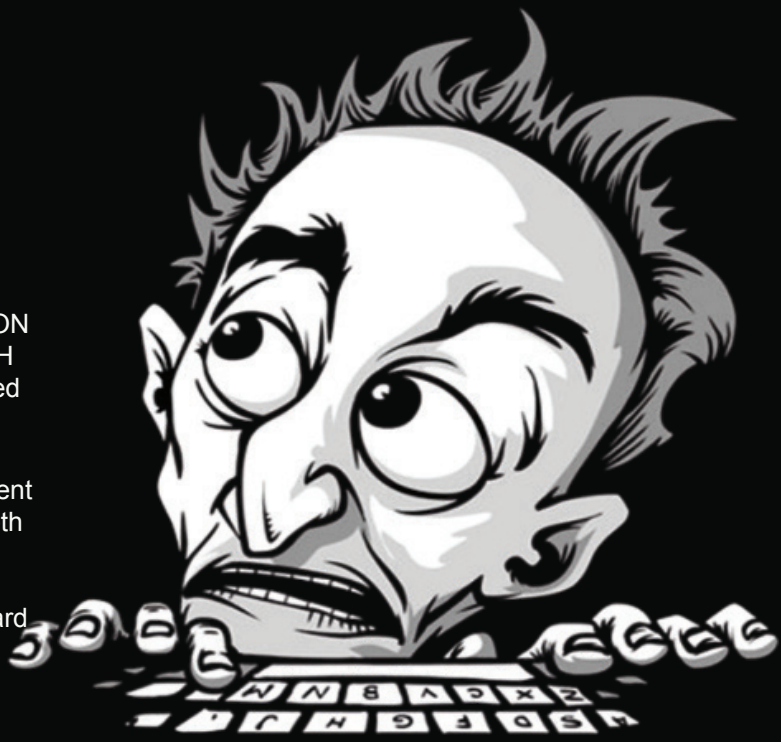
Twenty editions later, scale is still the least interesting part. People showed up, shared their work, asked questions, and passed enough energy forward for another room to follow.

A CONFERENCE BEGINS WHEN SOMEONE DECIDES THE ROOM IS WORTH BUILDING.

THE COUNT KEPT GOING.

ROOTCON held two editions in 2009. ROOTCON 2, Beers & Pongs, took place on 4 April at TOSH in Makati. ROOTCON 3, Pinoy Hackers, followed on 12 December at BayView Hotel in Manila.

The sequence matters. ROOTCON kept the event numbers and continued from there. The twentieth edition is the twentieth ROOTCON, not a claim about uninterrupted calendar years. Two rooms opened in one year, and the count moved forward with them.



TWO EVENTS. ONE YEAR. THE NUMBERING MOVED FORWARD.

BEERTALK





A CONFERENCE LEARNS TO MOVE.





By ROOTCON 4 in 2010, the conference was at Congo Grill in Ortigas, Pasig. ROOTCON 5 through ROOTCON 8 returned to Cebu at Parklane Hotel. ROOTCON 9 through ROOTCON 13 settled into Taal Vista in Tagaytay.

The venue changed, and with it the shape of the day: travel plans, after-hours conversations, how long people stayed, and how much room new activities could claim.

A venue is never the story by itself. It affects who can come, where strangers meet, and whether a quick question becomes a two-hour conversation. Each move created a different version of proximity.

Addresses tell only part of it. The living memory is in first arrivals, improvised fixes, long walks back after the program, and the moment an unfamiliar room finally sounded like ROOTCON. The conference learned to move because its people learned how to rebuild that feeling wherever they landed.

THE ROUTE SO FAR.

2008	**CEBU**	HANDURAW / RC1
2009	**METRO MANILA**	TOSH + BAYVIEW / RC2-3
2010	**METRO MANILA**	CONGO GRILL / RC4
2011-14	**CEBU**	PARKLANE / RC5-8
2015-19	**TAGAYTAY**	TAAL VISTA / RC9-13
2020-21	**ONLINE**	ZOOM + DISCORD + TWITCH / RC14-15
2022	**HYBRID**	ZOOM + TAAL VISTA / RC16
2023-24	**TAGAYTAY**	TAAL VISTA / RC17-18
2025-26	**CLARK**	ROYCE HOTEL / RC19-20

RECOVERY. REBOOT. HARD WIRE.



When COVID-19 shut borders and emptied venues, ROOTCON lost the room but not its reason for existing. RC14: Recovery Mode became the first fully virtual edition in October 2020. Talks moved through Zoom, conversations gathered on Discord, and Twitch carried the signal farther. The tools changed; the mission did not.

RC15: Rebooted remained online in 2021. The crew learned to moderate parallel spaces, rescue home connections, and recreate hallway help through a screen. It could not replace a crowded village or late-night conversation, but it kept the door open.

RC16: Hard Wire returned in 2022 as a hybrid event, joining Zoom Webinar with Taal Vista Hotel. Three editions proved that ROOTCON could change its format without surrendering its mission. When the room disappeared, the people kept the signal alive.





THE FILES ARE PART OF THE STORY.



The archive is not a victory lap. It is a workbench for memory. A slide deck can pull a forgotten argument back into the room. A speaker profile returns a voice to the stage. A contest result preserves a handle that might otherwise disappear. Photographs bring back the scale of the tables, cables, badges, and faces.

ROOTCON has carried pieces of itself forward from the first edition: talks, videos, profiles, contest results, photographs, and files people can still open, study, and pass around. Some years leave a dense trail. Others survive in a handful of stubborn fragments.

That unevenness makes the work human. Every missing caption invites someone to name a face. Every broken link asks whether another copy is sitting on an old drive. Preservation is not about freezing ROOTCON in place. It keeps the signal available for whoever comes looking next.

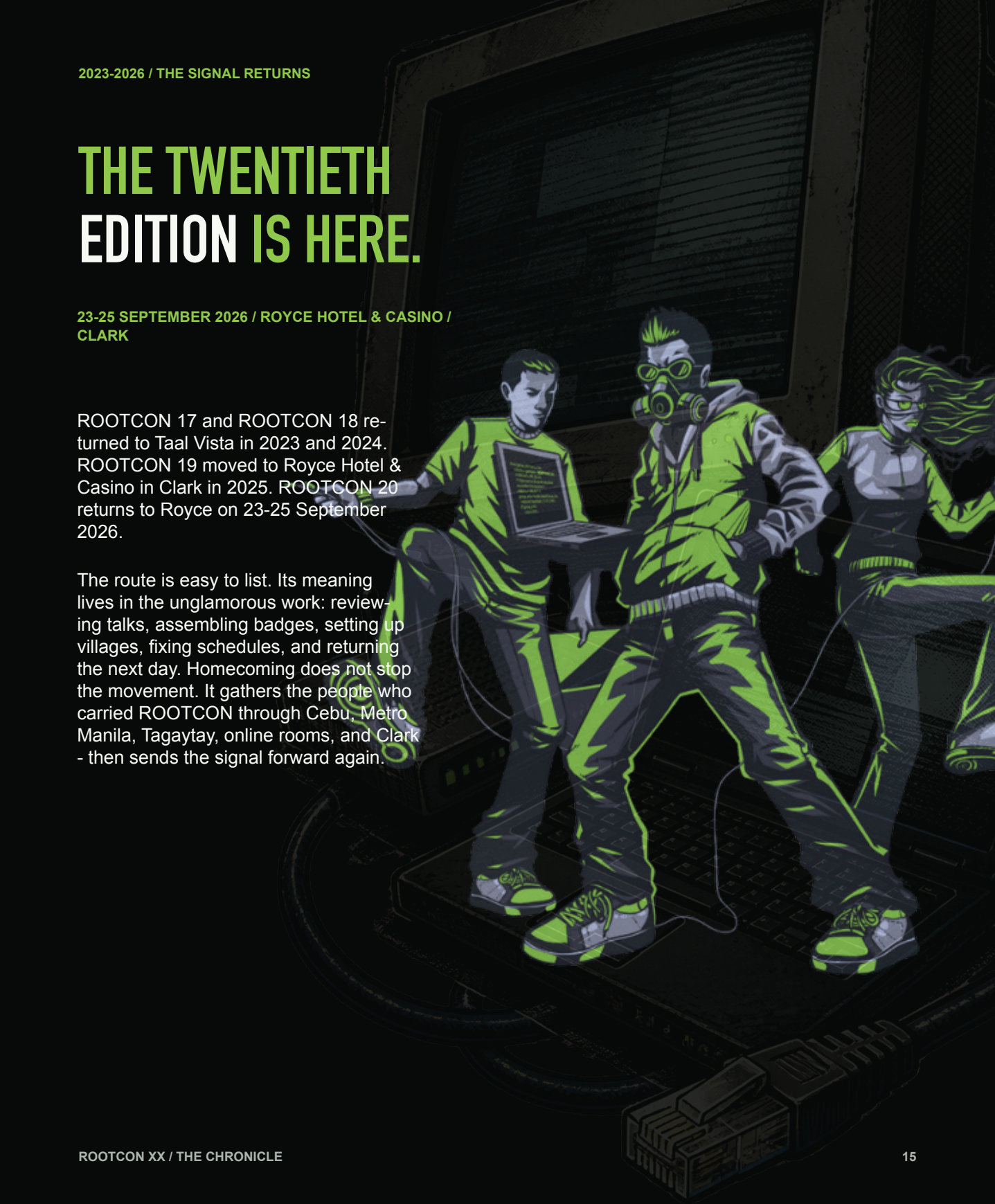
SAVE THE FILES. NAME THE FACES. KEEP THE SIGNAL MOVING. // MEDIA.ROOTCON.ORG

THE TWENTIETH EDITION IS HERE.

23-25 SEPTEMBER 2026 / ROYCE HOTEL & CASINO / CLARK

ROOTCON 17 and ROOTCON 18 returned to Taal Vista in 2023 and 2024. ROOTCON 19 moved to Royce Hotel & Casino in Clark in 2025. ROOTCON 20 returns to Royce on 23-25 September 2026.

The route is easy to list. Its meaning lives in the unglamorous work: reviewing talks, assembling badges, setting up villages, fixing schedules, and returning the next day. Homecoming does not stop the movement. It gathers the people who carried ROOTCON through Cebu, Metro Manila, Tagaytay, online rooms, and Clark - then sends the signal forward again.



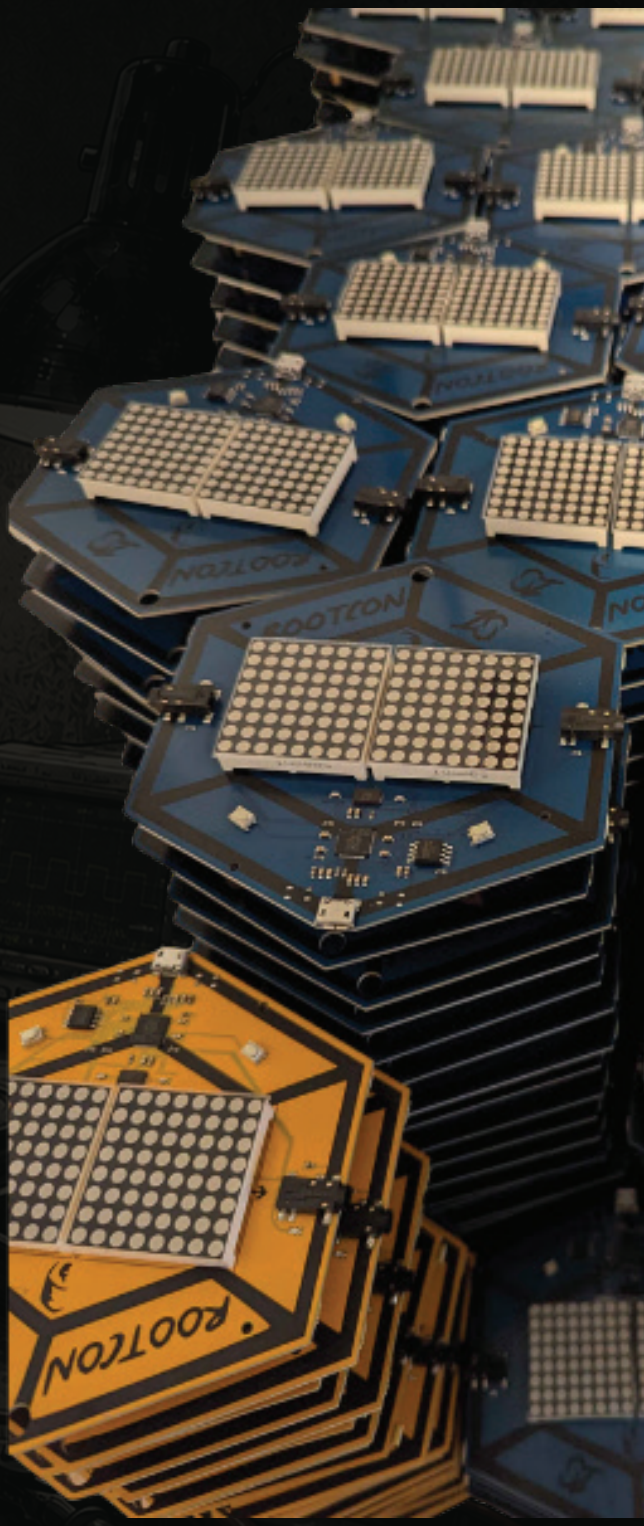
THE THINGS WE CARRY.

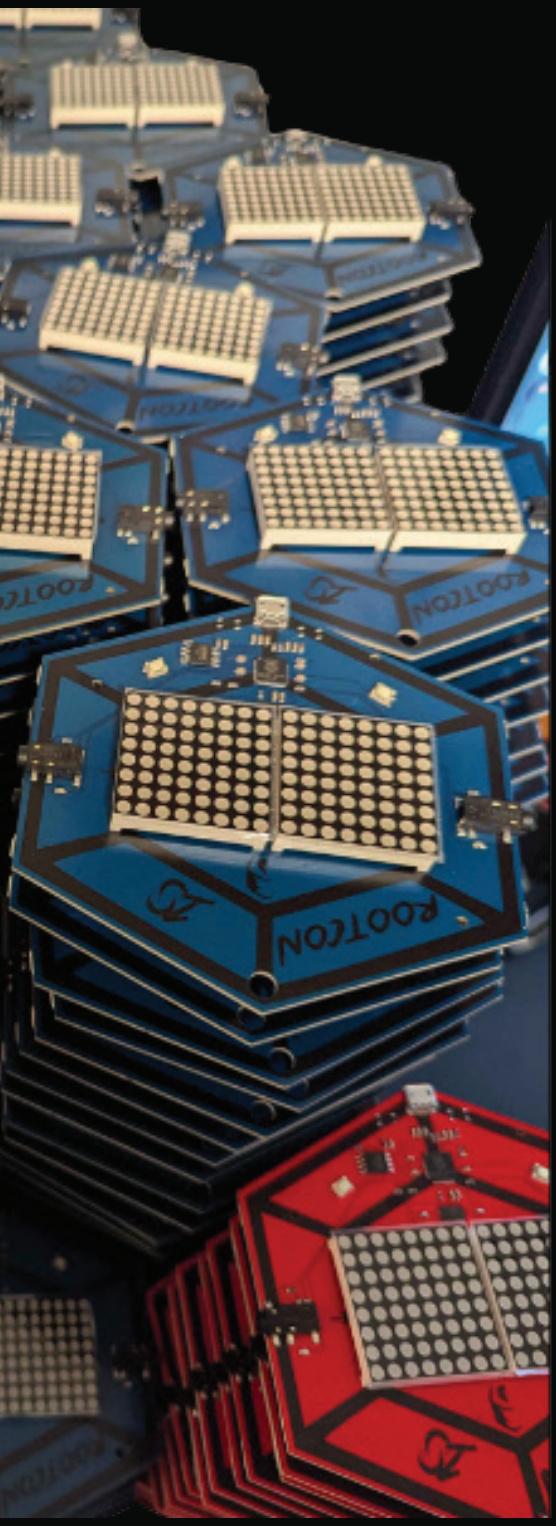
EVERY ROOTCON ARTIFACT TELLS A STORY

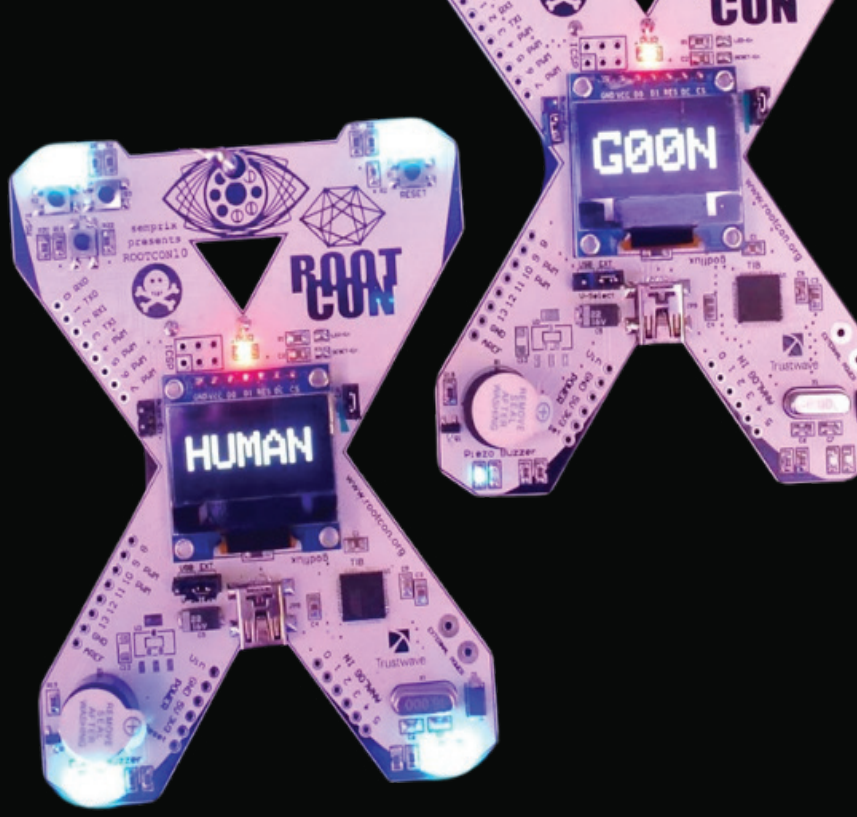
A conference leaves behind more than memories - it leaves the things people carry home. Badges, coins, stickers, shirts, lanyards, and tools become reminders of the ideas and encounters that shaped each edition.

Behind every object is a crew of makers: designers, engineers, developers, illustrators, fabricators, puzzle authors, volunteers, and sponsors. Their fingerprints remain in every revision, late fix, and stubborn detail that reaches the finished piece.

EVERY OBJECT REMEMBERS THE HANDS







A PASS BECAME A PLATFORM.

What began as a simple conference pass evolved into something far more ambitious. ROOTCON badges became interactive hardware—designed not only to identify attendees, but to be explored, modified, and hacked.

Each generation introduced new ideas: custom electronics, embedded firmware, RF communications, games, puzzles, hidden challenges, and collaborative experiences that continued long after the talks ended. No two badges were exactly alike, but they all shared the same philosophy: the badge should be part of the conference, not just proof of admission.

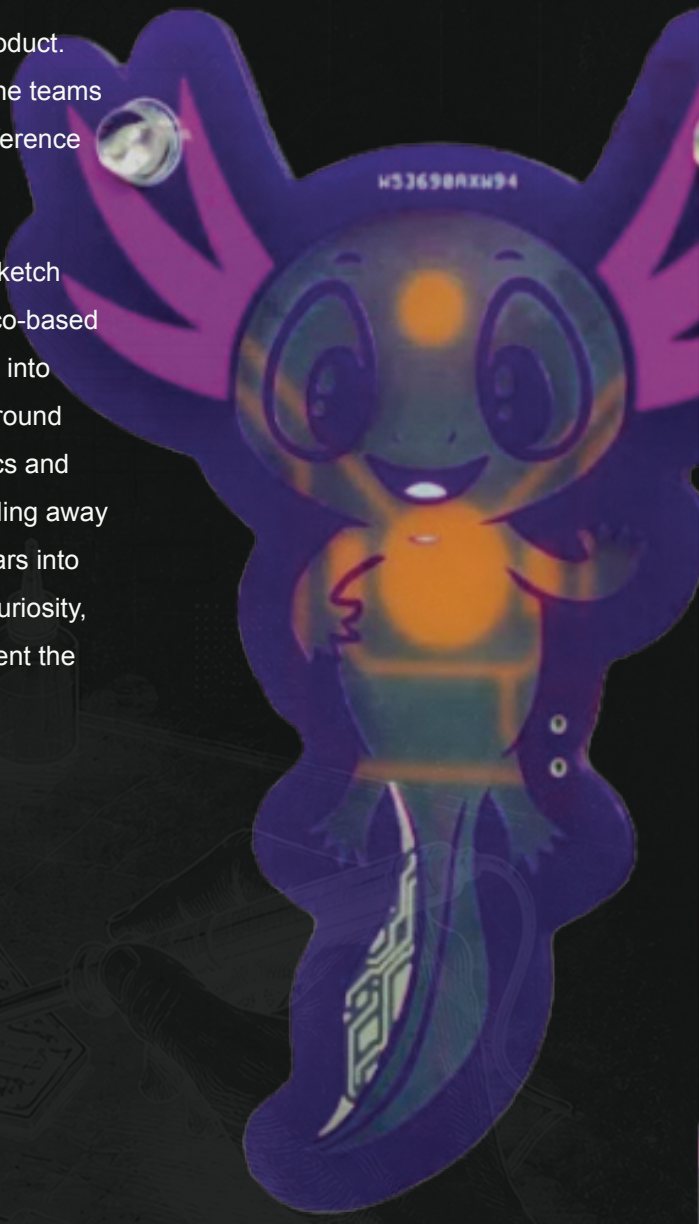
Today, a ROOTCON badge is more than a keepsake. It is a collectible, a conversation starter, a learning platform, and a snapshot of the creativity and ingenuity of the community that built it.

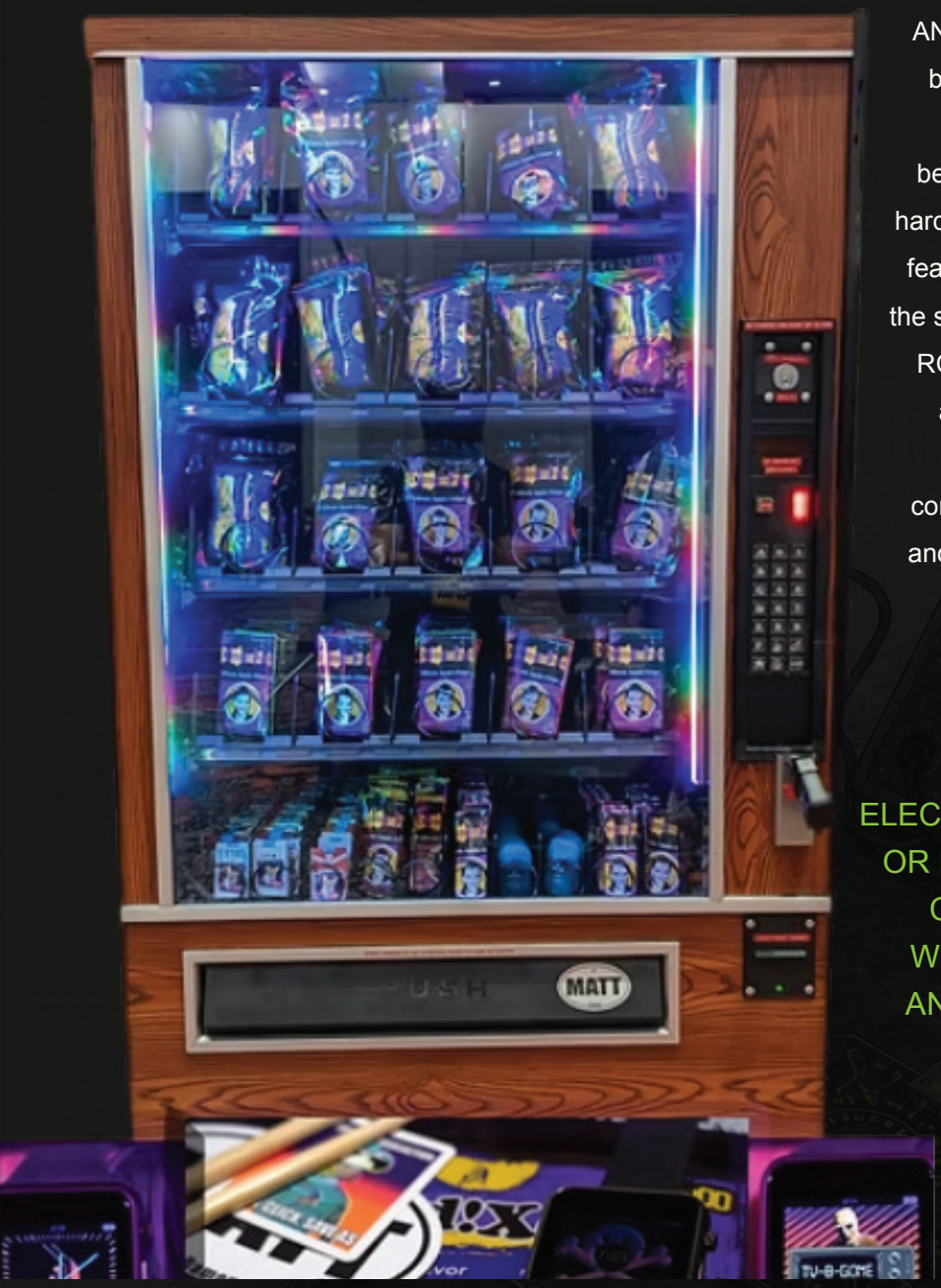
THE HANDS BEHIND THE BOARD.

Badge credits often disappear behind the finished product. This page puts them back where they belong - with the teams whose creativity, engineering, and craft turned a conference pass into a place to learn, collaborate, and play.

Electronic Cats enters the story when an ambitious sketch has to survive contact with manufacturing. The Mexico-based open-hardware team knows how to turn playful ideas into boards people can hold, power up, and take apart. Around ROOTCON, that means translating custom electronics and embedded systems into reliable badges without sanding away the invitation to experiment. Their best work disappears into the experience: the board boots, the features invite curiosity, and the attendee becomes part of the build the moment the tools come out.







AND!XOR approaches a conference badge like a compact world waiting to be opened. Custom PCBs, embedded software, radio, games, and hardware challenges are not separate features; they are different doors into the same object. The collective helped ROOTCON push its badges beyond admission and into participation. A board could carry a puzzle, start a conversation, reward a careful hand, and keep asking questions long after the conference lights went down.

ELECTRONIC CATS AND AND!XOR HELPED TURN THE ROOTCON BADGE INTO A PLACE WHERE ART, ENGINEERING, AND CURIOSITY SHARE THE SAME CIRCUIT.

SOME BUILDS COME BOTTLED.

HackSauce is one of ROOTCON's most unexpected creations—a collectible that blurs the line between novelty, tradition, and community. More than just a bottle of hot sauce, it embodies the conference's spirit of experimentation, where even the simplest idea can become a shared experience.

Produced in multiple editions, including the Original and Zombie Edition, HackSauce has become a recognizable part of ROOTCON culture. Like every well-crafted artifact, each bottle is the result of thoughtful design—from ingredient selection and recipe development to packaging, labeling, and production. Every detail reflects the same creativity and attention that goes into the conference's badges, puzzles, and challenges.



FIERY TASTE

Gideon is ROOTCON's friendly goat—curious, clever, mischievous, and always willing to wander where he probably shouldn't. Born from another ROOTCON curiosity and experiment, he embodies the community's habit of taking strange ideas seriously enough to build them, break them, improve them, and see where they lead.



MR. BLINKY BLING



The hands behind the ROOTCON 20 badge. Mr. Blinky Bling brings years of **#badgelife** hardware experience to our twentieth anniversary, turning the badge into something more than a conference credential.

THE FLOOR IS A LAB.

EIGHT COMMUNITY-RUN SPACES. EIGHT DIFFERENT WAYS TO STOP WATCHING AND START DOING.

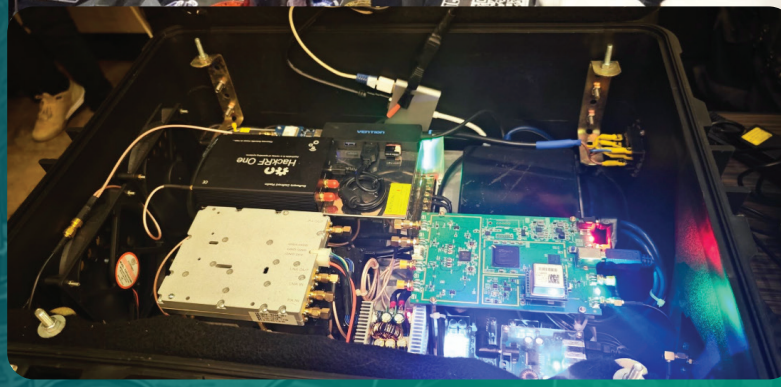
Villages are where the conference stops behaving like a row of chairs. Tools come out. Questions get specific. Someone hands you a board, a lock, a signal, or a problem with enough guidance to begin.

Each space is built by practitioners who choose participation over distance. Arrive curious, ask carefully, and leave with a skill that did not belong to you that morning.

Across RC20, eight community-run spaces turn the floor into a working lab. Different subjects, same invitation: step closer and join in.

EVERY VILLAGE BEGINS WITH CURIOSITY





Whether you're drawn to hardware, wireless, bug bounties, lockpicking, car hacking, reconnaissance, red teaming, or survival, each village offers a place to learn by doing. Some attendees arrive as experts. Most arrive with questions. Everyone leaves with a story.

Choose the subject that interests you. Stay long enough, and you'll discover the rest.



BUG BOUNTY VILLAGE

BUG BOUNTY + RESPONSIBLE DISCLOSURE

Bug Bounty Village Philippines is a community space for learning how responsible vulnerability research works from first reconnaissance to a report another human can act on. Talks, workshops, demonstrations, and collaborative discussions cover the methods, tools, and judgment needed to find weaknesses in real applications without losing sight of scope, evidence, or disclosure. The table is open to first-time hunters and experienced researchers sharpening their process. The point is not simply to find a bug. It is to understand the system, validate the impact, document the work clearly, and help make the digital ecosystem safer.

CAR HACKING VILLAGE

AUTOMOTIVE SECURITY + CAN BUS

Modern vehicles are networks with wheels, radios, sensors, and computers that must continue working under real-world pressure. Car Hacking Village turns that complicated system into something attendees can inspect safely. Through talks, workshops, hands-on labs, and CTF-style challenges, participants encounter electronic control units, in-vehicle networks such as CAN Bus, automotive protocols, and the attack-and-defense thinking used in vehicle security research. The environment is controlled and the boundaries matter. The aim is to understand how connected vehicles fail, how researchers test them responsibly, and how better evidence can lead to more resilient systems.

CELLULAR ASSAULT VILLAGE

CELLULAR NETWORKS + SIGNAL ANALYSIS



Cellular networks remain mostly invisible until someone examines the signals, protocols, infrastructure, and assumptions holding them together. Cellular Assault Village grounds that territory through demonstrations, discussions, and hands-on activities. Participants explore network operation, attack paths, and responsible assessment. Topics include signal analysis, mobile reconnaissance, protocol security, infrastructure risk, and defensive measures, with legal and ethical boundaries kept in view.

DOOMSDAY PREPPING VILLAGE

EMERGENCY READINESS + RESILIENCE



Doomsday and Emergency Preparedness Village is less interested in apocalypse theater than in useful decisions made before something goes wrong. It covers disasters, infrastructure failures, and other emergencies through planning, communication strategies, emergency kits, situational awareness, and resource management. Demonstrations connect individual preparation with community resilience. The objective is simple: build practical habits early enough that a bad day does not make every decision for you.

HARDWARE HACKING VILLAGE

ELECTRONICS + EMBEDDED MAKING

Hardware Hacking Village is where the abstraction ends and the board lands on the table. Participants work through electronics basics, soldering, Arduino programming, ESP32 projects, prototyping, and practical hardware-hacking concepts using approachable tools. The village makes its case through practice: useful hacking tools and research platforms do not require a perfect laboratory or unlimited budget. Affordable components, patient troubleshooting, and a willingness to build the first rough version can take an idea surprisingly far.

LOCKPICK VILLAGE

PHYSICAL SECURITY + LOCK SPORT

Lockpick Village brings security back to the physical layer. Firewalls and endpoint controls matter, but they cannot compensate for a door, cabinet, or rack that gives way without much argument. In a controlled hands-on setting, attendees learn how common locks operate, how bypass techniques expose weak assumptions, and what makes a locking system more resilient. Physical access can turn a carefully hardened system into reachable hardware, giving defenders and assessors a more complete view of risk beyond the network cable.

RED TEAM VILLAGE

ADVERSARY SIMULATION + LIVE CHALLENGES

Red Team Village is built around the attacker mindset, but the useful outcome belongs to both sides of the exercise. Presentations and live challenges give red teamers room to practice while helping blue teamers understand the paths an adversary may take. RC20 includes an OSINT Challenge and the return of the live Privilege Escalation Challenge with a new twist. Everything happens in a controlled environment where the objective is learning: follow the evidence, test the path, and understand what a defender needs to see in time.

RECON VILLAGE PH

OSINT + CYBER THREAT INTELLIGENCE

Recon Village PH focuses on the work before a technical engagement: collecting, validating, and interpreting information. Through OSINT, social engineering, and cyber threat intelligence, attendees explore how public data can reveal people, organizations, infrastructure, and patterns of behavior. Topics include digital footprinting, infrastructure discovery, online investigations, adversary profiling, and social-engineering psychology. Attackers and defenders use reconnaissance differently, but both need the same discipline: know what the evidence says, know what it does not, and do not turn a weak clue into a confident conclusion.

ENTER CURIOUS. LEAVE USEFUL.

A village is not a booth you walk past. Ask what is running, wait for the reset, follow the safety instructions, and make room for the person behind you. The fastest way in is usually a specific question.

01 / ASK BEFORE TOUCHING

Some rigs are live, fragile, sharp, hot, or mid-demo. A ten-second check prevents a long repair.

02 / STAY INSIDE SCOPE

Use the target, network, vehicle, lock, signal, and data provided for the exercise. Controlled means controlled.

03 / SHARE THE TABLE

Take your turn, then open the space. Villages work when beginners and veterans can both reach the tools.

04 / PROTECT THE EVIDENCE

Do not expose private data or photograph sensitive material. Ask before recording people or screens.

05 / RESET THE STATION

Return tools, clear the target, and tell staff what changed. The next participant should inherit a working problem.

06 / CREDIT THE BUILDERS

Ask who designed the challenge, built the rig, wrote the tool, or taught the technique. Names keep community work visible.

LEAVE WITH SOMETHING YOU CAN USE.

The best village moment rarely arrives with a stage introduction. It starts with: Can I try that? Someone makes room. A tool changes hands. The explanation becomes a demonstration, then a mistake, then a better question.

That exchange is the program. The equipment matters. The people willing to share it matter more.



CONTESTS + EXPERIENCES

THE CONFERENCE BECOMES THE GAME

Some people come to ROOTCON intending to sit still. This section is for everyone who eventually fails at that.

The contests turn the conference into a live system: screens become scoreboards, cables become race material, forgotten trivia becomes currency, and an ordinary hallway can become part of a clue. Technical depth matters, but so do observation, nerve, timing, teamwork, and the ability to laugh when the tester says no.

Play hard and keep the boundaries clean. Respect the organizers, the equipment, the venue, and the people sharing the floor. A win is worth remembering. A good game gives everyone a story.

THE RUNNING ORDER

01 CAPTURE THE FLAG

Break systems. Find flags.

02 CRIMP OR DIE

Build clean before time runs out.

03 HACKER KARAOKE

Take the mic and own the room.

04 HACKER JEOPARDY

Recall, wager, survive the board.

05 WI-FINDERS

Map signals without crossing lines.

06 SPOT THE FEDS

Observe first. Accuse carefully.

07 CODE BREAKERS

Follow clues across the con.

08 BREAKOUT PHILIPPINES

Escape-room instincts join the trail.

CAPTURE THE FLAG

EXPLOITATION + REVERSING + FORENSICS

ROOTCON's CTF puts teams in front of a scoreboard and problems designed to resist the first answer. Web exploitation, cryptography, reverse engineering, forensics, and binary work all have a way of appearing before the clock becomes friendly. Some flags fall quickly. Others follow a team home in spirit. The rhythm is simple: inspect the evidence, test an idea, share the useful discovery, and submit only what your team earned. The board remembers every solve, but the better reward is the moment a stubborn system finally explains itself.



CRIMP OR DIE

CABLE CRAFT + SPEED UNDER PRESSURE

Crimp Or Die reduces networking to eight conductors, one connector, and a clock that suddenly feels personal. Participants strip, order, seat, and crimp a working T568B cable using the supplied tools and materials. Speed helps, but the tester has no interest in confidence, excuses, or dramatic technique. A cable either passes or it does not. Early rounds narrow the field before the contest follows the survivors toward its Zero Hour finish. It is practical, loud, and wonderfully unforgiving: build clean, test green, and try not to donate another connector to the floor.



HACKER KARAOKE

ONE MICROPHONE + FIVE BRAVE MINUTES



Hacker Karaoke gives one attendee, one microphone, and one song enough room to become conference history. No professional training is required. Commitment helps. Performers choose from the official list, step into a short solo slot, and try to make the room come with them. Crowd energy counts, but respect matters more: keep the act safe, leave harassment outside, and treat the equipment and the next performer properly. Some voices land perfectly. Some arrive with more courage than pitch. Both can own the room. If a tie survives, the sing-off settles it.

HACKER JEOPARDY

TRIVIA + WAGERS + PUBLIC CONSEQUENCES



Hacker Jeopardy is what happens when years of security trivia, internet history, ROOTCON lore, movies, games, and suspiciously durable facts are placed on one board. Teams choose, answer, wager, and discover how quickly certainty disappears under stage lights. Fast recall earns points. A reckless wager can erase them. Wrong answers are not wasted; they become material for the hallway and sometimes survive longer than the winners. The contest works because the room participates too, leaning into every confident guess and every spectacular miss. Know the category, trust the teammate, and respect the buzzer.

WI-FINDERS

WIRELESS DISCOVERY + DISCIPLINED RECON

Wi-Finders turns the air around the conference into a field notebook. Participants discover and document unique wireless access points, building a picture of the signals already present without connecting to them, cracking them, or interfering with anyone's network. The work is reconnaissance in its cleanest form: listen, identify, record, and move responsibly. Antennas attract questions. Good boundaries answer them. Stay out of restricted spaces, follow local rules, and let the submitted BSSIDs tell the story. The winning total matters, but disciplined collection is the part worth carrying into real work.



SPOT THE FEDS

OBSERVATION + CLUES + HEALTHY SUSPICION

ROOTCON has always rewarded curiosity. Spot The Feds gives that curiosity a target. Designated players move through the conference while attendees study clues, behavior, badges, timing, and whatever else suddenly appears important. The goal is deduction, not harassment: make the call, accept the result, and let everyone keep enjoying the event. Goons sit this one out, and each successful spot closes one part of the hunt. Most people in the room are not the Fed. That has never stopped a hallway theory from growing legs. Watch carefully, ask cleanly, and do not poke every bear you meet.



CODE BREAKERS

ALTERNATE REALITY + CONNECTED PUZZLES

Previously called the Mystery Challenge, Code Breakers turns the conference into part of the puzzle. Digital clues lead toward physical objects; cryptography meets forensics; ordinary conversations start sounding suspicious. The trail rewards teams that notice what everyone else walks past and can connect fragments without forcing the story. RC20 adds a collaboration with Breakout Philippines, extending the challenge beyond a single screen. Follow the clue, break the code, check the assumption, and keep moving. The fastest team matters, but clean reasoning is what gets a team to the end.

BREAKOUT

BREAKOUT PHILIPPINES + PHYSICAL PUZZLECRAFT

Breakout Philippines brings its escape-room instincts into RC20's Code Breakers collaboration. The contribution is not another screen full of prompts. It is a reminder that puzzles can live in objects, spaces, timing, and the way a team communicates when the obvious route stops working. Details matter. So does restraint: observe before forcing, share what the team sees, and treat every strange element as intentional until the trail proves otherwise. Together, Code Breakers and Breakout Philippines turn the solve into something participants have to move through, not merely click through.

THE SCOREBOARD ENDS. THE STORY DOESN'T.

COMPETE CLEAN. LOSE LOUDLY. COME BACK READY.

A contest compresses the conference into a few sharp minutes. The cable works or it does not. The flag submits or it refuses. The answer arrives before the buzzer, the clue clicks into place, or the room decides the song belongs to everyone.

Then the score freezes. Tools go back into bags. Someone explains the mistake that cost the round, and another person realizes that explanation is exactly what they came to learn. That exchange is the real continuity between the contests: skill becomes story, and story becomes an invitation to try again.

Take the win without turning it into a throne. Take the loss without wasting it. Thank the people who built the game, help the next participant find the door, and carry the useful part home.

LEAVE THE GAME BETTER

PLAY INSIDE THE RULES.

RESPECT THE CREW AND THE EQUIPMENT.

SHARE THE LESSON, NOT THE FLAG.

LOOK AFTER THE ROOM.

TAKE THE STORY HOME.

TALKS + SPEAKERS

THE WORK ARRIVES WITH A VOICE

A conference talk begins long before the microphone goes live. It starts in a lab at an unreasonable hour, in an incident nobody expected, in a packet capture that refuses to make sense, or in a piece of hardware that finally gives up its secrets.

The people in these pages did the slow part first. They tested assumptions, broke tools, rebuilt methods, followed evidence, and kept notes worth sharing. ROOTCON gives that work a room - and gives the room permission to question it.

Read the roster, mark the talks that unsettle your current model, then show up ready to listen. The best session is rarely the one that ends at the final slide. It is the one that follows you into the hallway and changes what you try next.

26 SPEAKERS / 21 TALKS

01 AI + OFFENSIVE OPERATIONS

02 MALWARE + THREAT INTELLIGENCE

03 HARDWARE + EMBEDDED SYSTEMS

04 CLOUD + IDENTITY

05 TELECOM + RADIO

06 RED + PURPLE TEAMING

07 SPACE + CRITICAL INFRASTRUCTURE

08 CTFS + OPEN-SOURCE CRAFT



ADEN YAP

OFFENSIVE SECURITY + AI SUPPLY CHAINS

A lead penetration tester based in Malaysia, Aden has spent more than a decade breaking applications and infrastructure across industries. His research and disclosure work has produced 18 CVEs, backed by the same practical curiosity he brings to red-team engagements.



ALEX BAZHANIUK

HARDWARE + FIRMWARE + SUPPLY CHAINS

Alex is the CTO of Eclypsium and a longtime hardware, firmware, and supply-chain security researcher. Across more than 15 years, he has built research and product teams focused on the parts of computing that remain powerful, trusted, and too often overlooked.



ALTAF SHAIK

5G + TELECOM + WIRELESS SECURITY

Dr. Altaf Shaik researches telecommunications security at Technische Universitat Berlin. His work spans 5G and 6G architecture, Open RAN, embedded systems, and offensive network testing, with findings that have helped expose weaknesses in real mobile networks and standards.



ARIZ SORIANO

RED TEAMING + COMMUNITY BUILDING

Ariz leads the Theos Red Team and works across incident response, penetration testing, and adversary simulation. He also develops security learning content and founded ROOTCON's Red Teaming Village, turning field experience into tools and spaces where others can practice.



ARTEM DANILOV

EMAIL SECURITY + PARSER RESEARCH

Artem studies banking systems, mobile and web applications, and open-source business software. His vulnerability research has produced more than 20 CVEs. Recent work examines how mail gateways and clients disagree about MIME, creating room for malicious attachments to slip through.



ARV ARVANDY

ADVERSARY SIMULATION + AI-ASSISTED IDES

Arv is an offensive security practitioner with more than a decade in red teaming, advanced exploitation, and intrusion emulation. His work crosses software, databases, networks, agent-based systems, and the new attack surfaces created by AI-assisted development environments.



DAVIS ZHENG

THREAT INTELLIGENCE + SPACE SYSTEMS

Davis works in cyber threat intelligence, large-scale actor investigations, and security operations. His research reaches from information warfare and national security to space systems, where small computers, exposed interfaces, and mission-critical constraints make careful threat modeling essential.



DOAN MINH LONG

MALWARE ANALYSIS + THREAT TRACKING

Doan Minh Long is a threat analyst focused on reverse engineering, malware analysis, and tracking operators active in Southeast Asia. He follows campaigns from packed samples and loaders through infrastructure and attribution, turning technical fragments into a coherent operational picture.



DUC KIEN NGUYEN

REVERSE ENGINEERING + MALWARE

Duc Kien Nguyen is a malware analyst at Viettel Cyber Security and a longtime ARESx CTF member. He specializes in unpacking and reversing heavily obfuscated malware across native, Android, and .NET targets, and builds tools that help other analysts do the same.



EDO MALAND

RED TEAMING + ACTIVE DIRECTORY

Edo is a senior offensive security consultant with more than a decade in penetration testing, adversary simulation, and Active Directory security. He leads complex offensive engagements and has authored widely used open-source tools including TheFatRat, Sudomy, Brutal, and Vegile.



ELLWOOD THEWOOD

OFFENSIVE SECURITY + BADGE MAKING

Ellwood's path runs from systems administration and language work to penetration testing, electronics, radio, and technical surveillance countermeasures. He also builds electronic badges and CTF challenges, where hardware, play, and the satisfaction of a stubborn solve meet.



HEBE AU

RED TEAMING + AI SECURITY

Hebe is a senior offensive security consultant working across red teams, cloud, infrastructure, web, mobile, API, and wireless testing. Her current research follows adversarial machine learning and the practical failure modes that appear when AI systems meet enterprise software and human decisions.



im10n MIKHAIL

FREEIPA + ATTACK-PATH ANALYSIS

Mikhail developed IPAHound, a graph-based security analysis tool for FreeIPA. His work maps trust, delegation, host compromise, and identity relationships into visible attack paths, helping operators understand how one edge in a directory can become the route to wider control.



JUN MIURA

RED TEAMING + LOCAL LLMS

Jun is a red-team consultant and researcher at Fujitsu, specializing in offensive security and AI systems. His recent work studies how local language models can be used - and abused - from an attacker's perspective while keeping sensitive engagement data inside controlled environments.



OMKAR MALI

HARDWARE + OT + FIRMWARE

Omkar is a security researcher working across infrastructure, cloud, hardware, IoT, automotive systems, radio protocols, and firmware reverse engineering. He leads The Marathi Hackers Group and brings a teardown-first approach to devices trusted deep inside operational environments.



PENGFEI YU

PURPLE TEAMING + ADVERSARY EMULATION

Pengfei is an APJ and SAARC solutions architect at Picus Security. His background includes government red-team work and leading continuous purple-team implementation, giving him a close view of what turns threat intelligence into safe tests - and what reduces it to checkboxes.



PRIYA PATEL

THREAT HUNTING + APT RESEARCH

Priya works with SEQRITE Labs on security research and threat hunting. She follows advanced threat groups and real-world incidents across regions, connecting delivery chains, custom loaders, cloud infrastructure, and attribution clues into research defenders can act on.



RICK WESSON

SECURITY + MATHEMATICS + OPEN SOURCE

Rick has been on the network since 1988. He is a pilot, a farmer, a security practitioner, and an unapologetically human writer. His current experiment uses AI to recompose an open-source engine around ideas that once looked impractical to build alone.



SALIMAH LIYAKKATHALI

INCIDENT RESPONSE + THREAT INTELLIGENCE

Salimah works in global incident readiness and response, with a focus on cyber threat intelligence. Her earlier research examined threats to industrial control systems and critical infrastructure. She also teaches, investigates independently, and brings evidence from live cases back to the room.



SMRITI GABA

HARDWARE HACKING + RF SECURITY

Smriti is a senior security researcher working on next-generation EV charging infrastructure. Her experience spans hardware hacking, IoT, embedded systems, automotive security, and RF exploitation across drones, routers, smart meters, ECUs, and mobile communications.



SUBHAJEET SINGHA

MALWARE + ADVANCED THREAT RESEARCH

Subhajeet is a senior researcher at Acronis TRU Labs, working in threat intelligence, malware research, and reverse engineering. He investigates advanced campaigns, dissects custom tooling, and turns infrastructure, targeting, and code into detection guidance with operational context.



SUNGGWAN CHOI

ADVERSARY SIMULATION + MALWARE DEVELOPMENT

Sunggwan is an in-house red-team operator focused on adversary simulation, hands-on operations, malware development, and AI-assisted automation. He also co-founded RedRaccoon, a South Korean offensive security community built around meetups, competitions, and freely shared wargames.



TAKAO HOMMA

GENERATIVE AI + THREAT HUNTING

Takao is a security researcher and infrastructure engineer at Fujitsu Defense and National Security. He develops generative-AI threat-hunting tools for restricted environments, optimizing local language models where confidentiality, control, and repeatable evidence matter more than cloud convenience.



YEONWOO PARK

RED TEAMING + ACTIVE DIRECTORY

Yeonwoo performs penetration testing across SK Group affiliates and researches offensive methods with the SaturnX CTF team. His main interests are red teaming and Active Directory security, especially trusted mechanisms that can be bent into unexpected routes for access and persistence.



YI TING SHEN

AI RED TEAMING + SECURITY ENGINEERING

Yi Ting is a GenAI security researcher working on AI red teaming and security-focused applications. Their research combines practical engineering with evaluation of emerging systems, vulnerability discovery, and methods for making fast-moving AI products safer without losing sight of how attackers actually work.



DHILLON 'l33tdawg' KANNABHIRAN

KEYNOTE / COMMUNITY + THE NEXT UNDERGROUND

His keynote follows the hacker underground from IRC channels and shared exploit code into the institutions, companies, and national capabilities it helped create - then asks what happens when AI gives independent builders disproportionate leverage again.

ROOTCON XX / KEYNOTE

BEFORE CYBERSECURITY BECAME A GLOBAL INDUSTRY, IT WAS A COMMUNITY.

A HOMECOMING - AND A CALL FORWARD

Before security had budgets, frameworks, and career ladders, it had IRC channels, underground forums, shared exploits, hallway arguments, and people pulling systems apart for the pleasure of knowing. Those communities did more than survive the industry's arrival; their tools and research became its foundation.

Today AI is shifting leverage back toward independent builders and small crews. The tools can reason, automate, and amplify, but the old questions remain: who stays curious, who shares, and who builds what comes next? The underground did not disappear. It scaled - and its next chapter will be written by communities again.

0-DAY AND N-DAYS IN AI/ML SUPPLY CHAIN FRAMEWORKS

ADEN YAP / TRACK 2

A field-tested look at high-severity flaws in Mage-AI and Dify. The research moves from reconnaissance and insecure defaults to broken access controls and zero-click code execution, then asks what defenders should inspect before AI infrastructure becomes ordinary production infrastructure.

BEYOND THE CHECKBOX: HOW TO ENGINEER EMULATIONS THAT ACTUALLY MATTER

PENGFEI YU / TRACK 1

Adversary emulation should test the detections an environment actually needs - not merely fire technique IDs until a dashboard turns green. This session turns threat reporting into prioritized, safe, repeatable tests and a decision model teams can reuse when tradecraft and operational risk collide.

BRIDGING TRUST TO ROOT: OFFENSIVE RESEARCH INTO INDUSTRIAL COUPLERS

OMKAR MALI / TRACK 2

A teardown of serial-to-Ethernet couplers used around renewable-energy systems. Flash extraction, firmware reversing, credential recovery, and exposed services reveal how a small bridge device can become a root foothold for telemetry manipulation, lost visibility, and movement deeper into operational networks.

BUILD YOUR RED TEAM AI CREW: ONE PROMPT VS FIVE AGENTS

ARIZ SORIANO + HEBE AU / TRACK 1

One strong prompt or a five-agent pipeline? Sixteen controlled builds compare orchestration approaches across offensive tooling, using the same scanners and evaluation rubric. The session replaces instinct with measured results on correctness, operational security, completeness, and time to a working implementation.

COUNTER STRIKE: WHEN ZIGBEE'S ANTI-REPLAY BECOMES THE ATTACK

SMRITI GABA / TRACK 2

A production Zigbee presence sensor meets the mechanism designed to stop replay. Passive key extraction and authenticated packet injection turn anti-replay state into a controllable denial of service - taking a trusted sensor offline and bringing it back without jamming or an obvious failure.

CTRL + FLOW + ESC: ESCAPING RED TEAM CHAOS

YI TING SHEN + ARIZ SORIANO / TRACK 1

Offensive teams rarely lack tools; they lose the thread between them. BountyFlow treats reconnaissance, validation, evidence, and reporting as one connected information system, preserving context across the operation so teams can reduce duplicated work, recover decisions, and act on the right signal.

FOLLOWING THE SHELL: FROM PACKED LOADER TO VSHELL

DUC KIEN NGUYEN + DOAN MINH LONG / TRACK 1

A campaign targeting enterprises across South and Southeast Asia is followed from Themida-packed loaders through obfuscation and a Go payload to Vshell infrastructure. Reverse engineering, campaign comparison, and internet scanning meet in one investigation - and end with practical detection and prevention guidance.

IN CLOUD WE TRUST: MODIFYING CSP AGENTS FOR C2

YEONWOO PARK + SUNGGWAN CHOI / TRACK 1

Trusted AWS, Azure, and GCP management agents already execute commands, transfer files, and tunnel traffic. This research modifies their open-source code into red-team payloads, demonstrates three proof-of-concept tools, and maps the host and network evidence defenders can use to see the abuse.

INSTANT YARA SIGNATURES

RICK WESSON / TRACK 2

An experiment in rewriting a signature engine in Go with AI assistance adds two ambitious capabilities: scanning streams and producing signatures of its own. The result is part open-source rebuild, part field note from the edge of human-directed software creation.

IPAHOUND: WALKING ALONG THE EDGES IN FREEIPA

im10n MIKHAIL / TRACK 1

IPAHound brings graph-based attack-path analysis to FreeIPA. The session follows trust between FreeIPA and Active Directory, delegation, compromised hosts, and directory architecture, showing how relationships become edges - and how those edges reveal routes an operator might otherwise miss.

KHMER SHADOW: A CAMPAIGN AGAINST CAMBODIAN MILITARY INTELLIGENCE

SUBHAJEET SINGHA / TRACK 1

A targeted espionage investigation traces precision lures, the custom NightForge loader, Havoc command-and-control, and infrastructure pivots aimed at Cambodian government institutions. The technical chain is paired with victimology, geopolitical context, attribution reasoning, and detection guidance for defenders.

LOTIDE UNLEASHED: WEAPONIZING THE ATTACK LIFECYCLE AGAINST AI-ASSISTED IDES

EDO MALAND + ARV ARVANDY / TRACK 2

AI-assisted IDEs read repositories, execute tasks, render active content, store chat histories, and open trusted tunnels. LOTIDE turns those legitimate features into an intrusion path spanning initial access, command execution, credential theft, persistence, exfiltration, and command-and-control - without custom implants.

OPERATION DRAGON WEAVE

PRIYA PATEL / TRACK 2

A previously undocumented espionage chain combines shortcut-file spearphishing, a Rust dropper, layered cryptography, fiber-based execution, sandbox checks, and Adaptix command-and-control transported through Azure storage. The talk connects delivery, loader engineering, infrastructure, and attribution to a China-linked operator.

QILIN BE KILLING IT

SALIMAH LIYAKKATHALI / TRACK 2

Qilin ransomware succeeds without needing the loudest brand. Real incident-response cases show an operation built on disciplined tradecraft, fast execution, and a clear reading of enterprise environments. The session follows how the group's tactics work in practice and how they continue to change.

RECONSTRUCTING RED TEAM ENGAGEMENTS: DEVELOPING YOUR OWN RED AGENT

JUN MIURA + TAKAO HOMMA / TRACK 2

Red Agent uses local language models to carry engagement knowledge into remediation and validation. By structuring logs, reports, and operational data for reuse, it reduces the manual work of reconstructing attack paths and gives human operators more room for higher-value decisions.

SECURING SPACE: THREAT ASSESSMENT FOR NANOSATELLITE COMPUTERS

DAVIS ZHENG / TRACK 1

CubeSats make space more accessible - and carry legacy code, exposed debug ports, and fragile communications into orbit. This session combines hardware-aware threat taxonomy with mission-risk analysis to show how pre-launch shortcuts can become post-launch compromise, and why secure design must start on Earth.

SEG FAULT: WHEN TWO EMAIL PARSERS DISAGREE

ARTEM DANILOV / TRACK 1

Mail gateways and mail clients do not always parse the same message the same way. Those disagreements can hide malicious attachments from inspection. The research examines MIME edge cases, SMTP proxy mistakes, real gateway bypasses, and the controls needed to close the gap.

THE GHOST IN THE RACK

ALEX BAZHANIUK / TRACK 1

AI security reaches below prompts and models into the racks that power them. Firmware, controllers, interconnects, UEFI, BMC, and IPMI create an inherited attack surface across modern accelerators and data-processing units. Model integrity, the talk argues, begins with the hardware beneath it.

THE SILENT THREAT OF IMSI-CATCHERS IN THE AGE OF 5G

ALTAF SHAIK / TRACK 1

Low-cost rogue cell towers remain effective even as 5G promises stronger identity protection. Drawing on recent regional incidents and network testing, this session shows where safeguards remain incomplete and offers operators, regulators, and responders a practical route toward detection and faster coordination.

USING AI FOR CTFS - AND CREATING AI-RESISTANT CHALLENGES

ELLWOOD THEWOOD / TRACK 1

AI can now help solve, submit, and even generate CTF challenges. This talk examines both sides: automation available to players and design techniques that test what machines still struggle to do, from prompt traps and alternate flags to physical-world tasks that demand a human hand.

THE MIC GOES QUIET. THE WORK DOESN'T.

The room empties. Slides become tabs. A tool gets cloned, an assumption gets challenged, and somebody tries the technique on a system that matters. That is where the program becomes useful.

Carry the lesson carefully. Credit the researcher. Test inside the lines. Share what holds up, and say plainly what does not. If a question remains open, keep it open long enough for someone else to enter.

ROOTCON has always run on that exchange: work made public, criticism offered in good faith, and knowledge returned to the community with sharper edges than it arrived.

A TALK IS A HANDOFF, NOT A FINISH LINE.

AFTER THE SESSION

WRITE DOWN THE CLAIM.

FIND THE EVIDENCE.

REPRODUCE WHAT YOU CAN.

ASK THE QUESTION.

CARRY THE CREDIT FORWARD.

KEYNOTE SPEAKERS

TWO BUILDERS. TWO SIGNALS FROM THE EDGE.



KEYNOTE 01

DHILLON 'l33tdawg' KANNABHIRAN

FOUNDER + CEO / HACK IN THE BOX

KEYNOTE / BEFORE CYBERSECURITY BECAME A GLOBAL INDUSTRY, IT WAS A COMMUNITY.

Dhillon Andrew Kannabhiran has spent years building rooms where hard technical work can travel. As founder and CEO of Hack In The Box, he has brought researchers, hackers, and defenders together across the Asia-Pacific security community. His contribution is the connective tissue around the research: a stage, an audience willing to challenge it, and a culture that keeps knowledge moving. At ROOTCON XX, he looks back at the grassroots communities that built modern security before it became an industry, then asks what independent builders will do with the leverage AI now puts in their hands.



KEYNOTE 02

DR. ALTAF SHAIK

TELECOM SECURITY RESEARCHER / TU BERLIN

KEYNOTE / THE SILENT THREAT OF IMSI-CATCHERS IN THE AGE OF 5G

Dr. Altaf Shaik works at the layer most people trust without seeing: the mobile network. At TU Berlin, his research spans 5G and 6G architecture, Open RAN, access and core networks, embedded systems, and offensive telecom security. His PhD work contributed to stronger 4G security standards while exposing weaknesses in commercial networks; later research has continued through 5G protocols, slicing, APIs, SIM and eSIM systems, and attack simulation. At ROOTCON XX, he brings that long view to IMSI-catchers - small, deceptive cell sites that test whether the protections promised by 5G are actually switched on.

CFP REVIEW BOARD

Before a talk reaches a ROOTCON stage, somebody has already read it closely, challenged the premise, checked the technical spine, and asked whether the room will leave with something useful. The CFP Review Board does that quiet work. Different disciplines meet at the same table, looking past polish for substance, fresh voices, and ideas with enough weight to survive questions.



DAX LABRADOR AKA SEMPRIX

CURATION + COMMUNITY

Semprix brings ROOTCON's long memory to the table, looking for technical weight, a clear voice, and enough spark to wake the room.



DAN DUPLITO

LEADERSHIP + OPERATIONS

Dan brings a practical eye shaped by systems work, security consulting, and executive leadership.



JERWIN CUASON

SYSTEMS + PHYSICAL SECURITY

Jerwin follows systems wherever they lead: code, databases, telecoms, privacy, hardware, physical security, and the devices in between.



SCOTT JARKOFF

THREAT INTELLIGENCE + BUILDING

Scott brings threat-intelligence strategy and a builder's instinct shaped by co-founding Praeryx and the creative community deviantART.



AARON NG

SECURITY ENGINEERING

Aaron brings the operational view of a systems engineer who advises organizations across the Middle East, Turkey, and Africa.



JAY TURLA

CAR HACKING + RESEARCH

Jay brings car-hacking research, hardware curiosity, and the practical instincts of a ROOTCON goon and village organizer.



RAYMOND NUNEZ

CONSULTING + EDUCATION

Raymond works where consulting and teaching meet, carrying lessons from finance, government, and telecoms into the graduate classroom.

SEVEN READERS. DIFFERENT DISCIPLINES. ONE SHARED JOB: FIND WORK WITH A PULSE, PUSH IT UNTIL IT HOLDS, AND MAKE ROOM FOR VOICES THE HALLWAY HAS NOT HEARD YET.

ZERØ-HOUR PARTY / THE CONFERENCE EXHALES. THE NIGHT KEEPS MOVING.





ZERO HOUR

DROP THE BADGE. RAISE A GLASS. FIND YOUR CREW. TURN UP THE VOLUME. WRAP UP ROOTCON THE ONLY WAY WE KNOW HOW.

THE TALKS END. THE HALLWAY GETS A SOUNDTRACK.



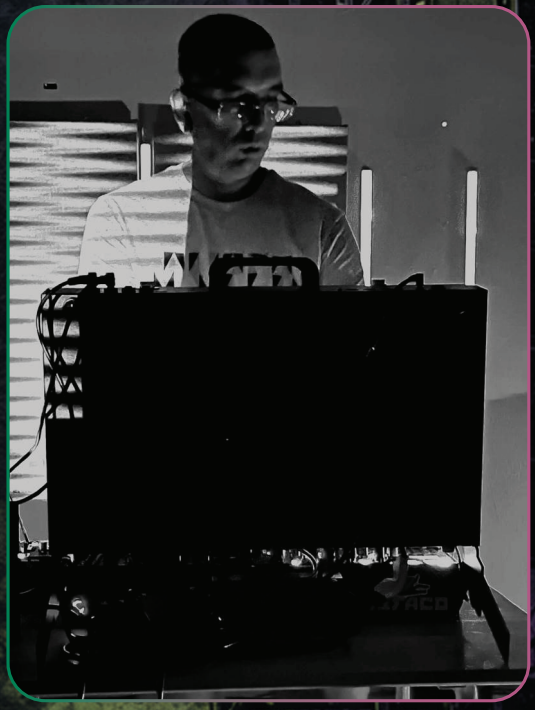
ASTRA

Four years on the ROOTCON stage, and Astra still knows how to keep the room alive. From familiar anthems to late-night chaos, they've become part of the soundtrack of ROOTCON.

When the talks end, the volume goes up. Dhillon "DHANKA" Kannabhiran trades the conference stage for the decks, bringing his energy from the hacker community straight to the ROOTCON floor. No slides, no demos—just beats, bass, and a proper way to close the night.

KNOW THE BEAT. TRUST THE CROWD. OWN THE NIGHT.

ASTRA × DHANKA



DHANKA

HOW DO YOU GAIN ACCESS TO EVERYTHING?

BENEATH THE SURFACE

Russian Reverse follows a century of Soviet and Russian reverse engineering through people who learned to understand technology by taking it apart.

The work begins with a finished program, machine, or device whose inner logic remains hidden. By dismantling it and tracing how its parts interact, an engineer can reconstruct both the mechanism and the thinking behind it.

The documentary connects that process to an old human instinct: looking beneath the surface. It demands curiosity, patience, and time. The film also carries an explicit national frame, presenting reverse engineering as a route toward technological independence - learning from existing systems before building new ones.

BEHIND THE FILM

Production took eighteen months: ten months of development followed by eight months of filming and post-production. The documentary was reworked three times to balance the language of practicing reverse engineers with the needs of a broader audience.

Filming moved through company offices, research laboratories, the Museum of Cryptography, the Museum of Military Vehicles, Cyberdom, and Motorika's production line.

PEOPLE INSIDE THE SYSTEMS

The crew documented bionic prosthetics, autonomous driving, specialist hardware tools, and systems usually hidden from public view. Contributors came from Positive Technologies, Kaspersky Lab, T-Bank, Rosatom, IVI, SR Space, Elverils, Motorika, museums, and historical projects.

The film's final question reaches beyond access: once we understand how a system works, what should we do with that knowledge?

EXPLORE THE HISTORY OF SOVIET & RUSSIAN REVERSE ENGINEERING

A CENTURY OF UNDERSTANDING TECHNOLOGY BY TAKING IT APART.

Directed by
VLADIMIR ARSHININ

RUSSIAN REVERSE



DIRECTED BY VLADIMIR ARSHININ
ORIGINAL IDEA BY DENIS BARANOV
CREATED BY POSITIVE TECHNOLOGIES

SPONSORS

ELITE + PLATINUM / SUPPORTING THE WORK BEHIND THE ROOM.

APPDOME

ELITE

Mobile-app defense against fraud, malware, account takeover, bots and identity threats.

appdome.com

ECLYPSIUM

PLATINUM

Protects enterprise firmware, hardware and software while monitoring device and supply-chain risk.

eclypsium.com

VIETTEL CYBER SECURITY

PLATINUM

Develops in-house cybersecurity solutions for governments, large organizations and SMEs.

viettelsecurity.com

QUALYS INC

PLATINUM

Cloud security and compliance for asset visibility, risk prioritization and remediation.

qualys.com

THEOS CYBER

PLATINUM

APAC partner delivering cyber defense, offense and response for regulated organizations.

theos-cyber.com

NEXUS

PLATINUM

Philippine IT provider with Orion-managed cybersecurity services for protection and response.

nexus-orion.com

NINJA ONE

PLATINUM

Unified endpoint management, autonomous patching, backup and remote access.

ninjaone.com

TECHNOPATH SOLUTIONS INC.

PLATINUM

Philippine provider of cybersecurity, IT operations and managed services.

technopathsolutions.com

PLATINUM + GOLD

OFFICIAL RC20 TIERS, IDENTITIES AND PUBLISHED DESTINATION LINKS.

M-SECURITY TECH PHILIPPINES, INC.

Regional distributor of cybersecurity and network-performance solutions through reseller partners.

PLATINUM

mtechpro.com

GIGAMON

Deep observability using network-derived telemetry across cloud and security tools.

PLATINUM

gigamon.com

RT&CO. CYBERSECURITY, INC.

CREST-certified testing, SOC operations, monitoring, forensics and security consulting.

GOLD

rtcocyber.com

SANS INSTITUTE

Cybersecurity training and certification for practitioners, teams and organizations.

GOLD

sans.org/apac

YESWEHACK

Exposure management combining bug bounty and autonomous and continuous pentesting.

GOLD

yeswehack.com

NULLFORGE SECURITY INC.

Tailored cybersecurity services for organizations across diverse industries.

GOLD

nullforge.net

ELECTRONIC TRANSFER & ADVANCE PROCESSING INC.

Philippine self-service machines, software, integrations and managed operations.

GOLD

etap.com.ph

ESCAN

Endpoint security and XDR technologies distributed locally by Netplay.

GOLD

npi.ph/escan

GOLD + SILVER

SECURITY, TRAINING, INFRASTRUCTURE AND COMMUNITY SUPPORT.

OFFSEC

Cybersecurity education provider behind Kali Linux, OSCP and hands-on training.

GOLD

offsec.com

NCC GROUP

Global cybersecurity, business-resilience and software-escrow organization.

GOLD

nccgroup.com

GRAYBOX SECURITY

Managed, advisory, offensive-security, incident-response and compliance services.

GOLD

grayboxsecurity.com

KNOWBE4

Workforce security for training, attack simulation and AI-agent defense.

GOLD

novare.com.ph

RED ROCK IT SECURITY

Philippine threat management, risk reduction and cybersecurity talent development.

GOLD

redrocksecurity.io

PHILIT SYSTEM DESIGN SOLUTIONS CO.

Filipino digital-transformation company building custom cloud-based business applications.

SILVER

philitsolutions.com

HOLY ANGEL UNIVERSITY

Accessible education grounded in competence, conscience and compassion.

SILVER

hau.edu.ph

CYBLE

AI-native threat intelligence, digital-risk protection and autonomous security operations.

SILVER

cyble.com

SILVER

TECHNOLOGY, ASSURANCE AND OPERATIONAL DEFENSE.

SILVER

R.G. MANABAT & CO. (KPMG IN THE PHILIPPINES)

Philippine audit, tax, advisory and technology-consulting member firm.

home.kpmg/ph

SILVER

SOPHOS

Adaptive cyber defense combining AI analysis, prevention and integrated protection.

npi.ph/caas-sophos

SILVER

PICUS SECURITY

Continuous security validation combining attack simulation and automated pentesting.

picussecurity.com

SILVER

NETWORK MANAGER SALES INC

Philippine IT provider promoting Vonahi vPentest and business-security solutions.

nmiph.com

SILVER

NETPLAY

Philippine value-added distributor of enterprise IT and cybersecurity products.

npi.ph

THE ROOM IS BUILT TOGETHER.

ACKNOWLEDGEMENTS

A DRAFT MAP OF WHO MADE ROOTCON 20 POSSIBLE.

A conference is only the visible part. Behind every talk, village, contest, badge and late-night conversation is a long chain of people who planned, carried, checked, fixed, welcomed and stayed after the room had emptied.

ORGANIZERS + GOONS + VOLUNTEERS

The teams who shaped the program, answered questions, solved emergencies and kept the conference moving.

CONTENT

CFP reviewers, speakers and trainers who read closely, prepared deeply and shared work with the room.

VILLAGES + CONTESTS

Leads, builders, judges and crews who turned specialist knowledge into something people could touch and try.

OPERATIONS

Registration, safety, logistics, technical support and everyone carrying the unglamorous work between rooms.

VENUE + PRODUCTION

Hotel staff, stage crews, audio, lighting, documentation and production teams who made the temporary city function.

SPONSORS + PARTNERS

Organizations and community partners whose support helped keep research, learning and shared experiences accessible.

ARCHIVISTS + MAKERS

Photographers, writers, designers, badge makers and collectors who preserved the details that memory eventually drops.

ATTENDEES + HOME CREW

The people who filled the room - and the families, friends and colleagues who made it possible for them to be there.



THIS PAGE INTENTIONALLY LEFT BLACK.

FOR WORLD DOMINATION



Copyright © 2026 ROOTCON® Conference Inc. All rights reserved.