

Wednesday 27. September

2:00 PM

**2:00** Early Registration

PM  
3h

Please come to the foyer of the National Convention Centre to pick your pack up the day before the conference and beat the crowds

[Event Track](#)

Logistics

Thursday 28. September

9:00 AM

**9:00** 101 Keynote: Intro to BSides Canberra

AM  
25min

This talk covers the history and ethos of hackercons in Australia with some tips and advice on how to get the most out of the conference.

[BSidesCbr 101](#)

Royal Theatre

9:30 AM

**9:30** Locksport Village

AM  
7h30min

Get ready to immerse yourself in the captivating world of locksport. Our doors swing open each day from 10 am to 5 pm, welcoming all curious souls. Locks, tools, and seasoned instructors are at your disposal, so why not seize this golden opportunity to learn a trick or two from the experts?

...

[Event Track](#)

Locksport

**9:30** Black Bag

AM  
8h

 Redacted, Ty Ridgeway, Julian Abrahams

A black bag is a physical security competition where teams of participants attempt to capture intelligence (flags) from a physical environment without being detected.

Registration can be done here: <https://blackbag.redacted.au/>

[Event Track](#)

Blackbag Room

**9:30** Intro to Capture-the-Flag (CTF) Session 1

AM  
60min

 Cybears

A Capture-The-Flag (CTF) competition is a fun way to get started in the cyber security field, learn new skills and challenge yourself. However, it can be daunting, especially if you've never played before.

This session will be an introduction to CTFs, including how to get set-up, what tools you may like to use, and how you can go about solving challenges! It will walk through the different challenge categories and may...

[Event Track](#)

Hardware Village Stage

**9:30** A hacker's view of DoS attacks

AM  
55min

 David Robinson

This talk will go over the ways a hacker conducts reconnaissance against an organisation to select targets best suited for a DoS attack. Following that, we will provide methods for defending your organisation and web applications.

...

[BSidesCbr 101](#)

Royal Theatre

**9:30** Hardware & Wireless Village

AM  
7h30min

Bored with tcpdump? IDA got you down? Forget your neglected VMs, come hack hardware! Bring your RTL-SDR dongles, buspirates, and '80s phone phreaking kit - let's hack together!

Soldering irons will be available for all you tech wizards. You can use them to make badge modifications or for any other hardware hacks you have in mind. Need help with your conference badge? We've got your...

[Event Track](#)

Hardware & Wireless Village

**9:30** Careers Panel: CISO

AM  
45min

 Ricki Burke

This panel will feature top security executives who will share insights into their roles and discuss the current cybersecurity landscape.

[Event Track](#)

Careers Village

10:30 AM

**10:30** RF Demos

AM  
20min

 Amy Nightingale, John Gerardos

Radios are everywhere, and RF technology is applied in places that you might not even have thought of, and this usage is only going to grow. Come learn how basic Radio technology works, what you can transmit and receive, as well as the legalities you need to keep in mind before blasting the entire CBD with RF interference (hint: don't).

...

[Event Track](#)

Hardware Village Stage

**10:30** Career Village: What Is - Red teaming

AM  
30min

 Ricki Burke

Industry professionals will break down specialised areas of security, such as red teaming, penetration testing, and incident response etc, sharing the necessary skills, daily tasks, and advice on how to break into these fields.

[Event Track](#)

Careers Village

11:00 AM

**11:00** Careers Panel: Neurodiversity

AM  
60min

 Ricki Burke

Panel Discussion with Adam Foster

[Event Track](#)

Careers Village

**11:00** Designing a Badge Add-on in KiCad Day 1

AM  
2h

Josh Johnson

Ever wanted to design a PCB but unsure where to begin? This workshop will be a guided tour through designing a badge add-on in KiCad, concluding in assembly of the add-on which you can proudly attach to your conference badge to show off your newly acquired skills. Please bring a laptop with KiCad installed and a mouse to get the most out of the workshop.

[Event Track](#)


Hardware Village Stage

**11:00 AM**  
25min  
**Introduction to Malware Development in C#**  
Jayden Caelli  
Learn how to build basic malware in C# and how to bypass modern AV and EDR products.  
[BSidesCbr 101](#)  
Royal Theatre


11:30 AM

**11:30 AM**  
55min  
**Locks on the wire**  
Eldar Marcussen  
With the increased use of smart office technology there are more avenues to leverage software vulnerabilities to remotely control access to carparks, buildings, rooms, lockers, etc. In this talk we will explore a few solutions and some of the issues with these solutions and how they can be (ab)used.  
[Main Track](#)  
Royal Theatre


12:00 PM

**12:00 PM**  
30min  
**CV Workshop**  
 Ricki Burke  
Participants will learn how to create effective resumes and improve their chances of landing their desired roles.  
[Event Track](#)  
Careers Village

12:30 PM


**12:30 PM**  
60min  
**Careers: I'm hiring/networking**  
 Ricki Burke  
Attendees will have the opportunity to network with hiring managers seeking to expand their teams.  
[Event Track](#)  
Careers Village


1:30 PM

**1:30 PM**  
25min  
**Comprehending Kayfabe: a lens for dealing with cognitive hacking, online influence and layered deception**  
 Steven Coomber  
Cyberattack is about data and integrity not only network security, as breaches also effect an enterprise's values, reputation and brand. Cognitive hacking using dis-mis-mal-information is cyberattack aimed at manipulating perception and exploiting psychological vulnerabilities to change behaviour. This makes online influence campaigns across social media, the internet and networking infrastructure a cyber problem and solutions part of the cyber environment. We know disinformation can amplify social tensions and unsettle communities, but to what degree can it be intentionally weaponised on a population without it's knowledge?...  
[Main Track](#)  
Royal Theatre


**1:30 PM**  
45min  
**Careers Panel - How to Build Your Brand and Career in Cyber**  
 Ricki Burke  
Careers Panel  
[Event Track](#)  
Careers Village

2:00 PM


**2:00 PM**  
55min  
**Ethan Hunt on a Budget**  
 Tim Noise  
In the early ages of machine learning we've seen memes, misinformation and music videos. In this talk we look at the concepts of identity - specifically document verification and biometrics commonly used in sectors such as fintech, medical and other major sectors for online verification of identity. We tested (with permission) 4 major vendors in this space and highlight weak spots in both the technology, the concept of identity and call upon the machine uprising to use their own powers against them. live demos, fun and cause for concern.  
[Main Track](#)  
Royal Theatre


**2:00 PM**  
60min  
**Intro to Capture-the-Flag (CTF) Session 2**  
 Cybears  
A Capture-The-Flag (CTF) competition is a fun way to get started in the cyber security field, learn new skills and challenge yourself. However, it can be daunting, especially if you've never played before.  
This session will be an introduction to CTFs, including how to get set-up, what tools you may like to use, and how you can go about solving challenges! It will walk through the different challenge categories and may...  
[Event Track](#)  
Hardware Village Stage


2:30 PM

**2:30 PM**  
30min  
**Careers: What is - Incident Response**  
 Ricki Burke  
Industry professionals will break down specialised areas of security, such as red teaming, penetration testing, and incident response etc, sharing the necessary skills, daily tasks, and advice on how to break into these fields.  
[Event Track](#)  
Careers Village

3:00 PM

**3:00 PM**  
25min  
**APT Attack Techniques in Azure Cloud**  
 Lina Lau (@inversecos)  
Difficult to detect and pervasive in nature, cloud attack techniques attract the likes of APT groups like Nobellium who have increased their focus on abusing identity federation. Techniques like Golden SAML and AD FS skeleton keys provide threat actors the double-edged sword of combining both lateral movement and privilege escalation into a single technique – with the added benefit of leaving little trace in the cloud logs for defenders....  
[Main Track](#)  
Royal Theatre

**3:00 PM**  
20min  
**RF Demos**  
 Amy Nightingale, John Gerardos  
Radios are everywhere, and RF technology is applied in places that you might not even have thought of, and this usage is only going to grow. Come learn how basic Radio technology works, what you can transmit and receive, as well as the legalities you need to keep in mind before blasting the entire CBD with RF interference (hint: don't).  
...  
[Event Track](#)  
Hardware Village Stage

**3:00 PM**  
30min  
**Careers Village: What is - Application Security**  
 Ricki Burke, Artemis Calvi  
What is Application Security with Louis Nyffenegger  
[Event Track](#)  
Careers Village

3:30 PM

**3:30 PM**  
30min


**Job Market Update**  
A session providing an update on what the cyber security industry in Australia looks like in terms of jobs in the market and trends in the industry. I have been tracking this data for over nearly two years.

[Event Track](#)

Careers Village

4:00 PM

**4:00 PM**  
25min

**Case Studies in Point of Sale Hardware Hacking**  
 Zoi Petroulias

Point of sale devices are found in many retail outlets and handle sensitive financial, sometimes personal, information. They're easy to use and easy to reach. It literally pays to wonder, how are they protected? Sometimes there are locks to keep out curious customers, and many devices employ proprietary communications protocols as a barrier against less sophisticated signal sniffing attacks. I recently had the opportunity to conduct security assessments on a couple of such devices. In this talk, I'll explain what hardware hacking techniques I used to perform a black-box analysis of these devices. I'd expect any bad actor to do the same.

[Main Track](#)

Royal Theatre

4:30 PM

**4:30 PM**  
55min

**'Hold Your Horses'; Stopping A North Korean Supply Chain Attack Before It Bolts**  
CG

Supply chain attacks are bad. Supply chain attacks conducted by North Korea are worse.

This presentation provides a "view from the trenches" of how to confidently detect, analyse, and attribute activity conducted by the Democratic People's Republic of Korea (DPRK) adversary LABYRINTH CHOLLIMA...

[Main Track](#)

Royal Theatre

5:00 PM

**5:00 PM**  
2h

**HackerChix Networking Event**

For delegates identifying as women, please join us for a cocktail event on Level 1 in the Ballroom Foyer.


[Event Track](#)

Logistics

Friday 29. September

9:10 AM

**9:10 AM**  
55min

**Keynote: When Exploits Aren't Binary**  
 Maddie Stone

When Exploits Aren't Binary

[Main Track](#)

Royal Theatre

9:30 AM

**9:30 AM**  
7h30min

**Locksport Village**

Get ready to immerse yourself in the captivating world of locksport. Our doors swing open each day from 10 am to 5 pm, welcoming all curious souls. Locks, tools, and seasoned instructors are at your disposal, so why not seize this golden opportunity to learn a trick or two from the experts?

...

[Event Track](#)

Locksport

**9:30 AM**  
7h30min

**Hardware & Wireless Village**

Bored with tcpdump? IDA got you down? Forget your neglected VMs, come hack hardware! Bring your RTL-SDR dongles, buspirates, and '80s phone phreaking kit - let's hack together!


Soldering irons will be available for all you tech wizards. You can use them to make badge modifications or for any other hardware hacks you have in mind. Need help with your conference badge? We've got your...

[Event Track](#)

Hardware & Wireless Village

10:00 AM

**10:00 AM**  
20min

**RF Demos**  
 Amy Nightingale, John Gerardos


Radios are everywhere, and RF technology is applied in places that you might not even have thought of, and this usage is only going to grow. Come learn how basic Radio technology works, what you can transmit and receive, as well as the legalities you need to keep in mind before blasting the entire CBD with RF interference (hint: don't).

...

[Event Track](#)

Hardware Village Stage

**10:00 AM**  
7h30min


**HuntIR by ACSC**  
 ACSC

Do you want to try out your incident response skills for a day? Want to know what it is like to perform technical analysis when the pressure is on? Come and try the Australian Cyber Security Centre's Incident response game - HuntIR. HuntIR is an incident response game developed by the Digital Forensics Incident Response team that focuses on the analysis of technical artefacts to answer key investigation questions. Each player is given 24 hours to perform technical analysis on their own unique incident that includes various logs including process listings, autoruns, IIS access logs and more. Stay in regular contact with your victim organisation...

[Event Track](#)

Competition Room Stage 2

**10:00 AM**  
7h30min

**Black Bag**  
 Redacted, Ty Ridgeway, Julian Abrahams

A black bag is a physical security competition where teams of participants attempt to capture intelligence (flags) from a physical environment without being detected.

Registration can be done here: <https://blackbag.redacted.au/>

[Event Track](#)

Blackbag Room

**10:00 AM**  
7h30min

**CTF Mayhem Unleashed!**  
 Cybears

The Cybears will return to run the BSidesCBR 2023 Capture-The-Flag competition! A CTF is a competition where teams use their knowledge of computer and network security to solve challenges in a Jeopardy format. The challenges may cover topics such as web exploitation, binary exploitation, cryptography, reverse engineering and will include challenges for people just getting started in the industry as well as seasoned CTF players...

[Event Track](#)

Competition Room Stage 1

10:05 AM

**10:05 AM**  
25min

**Introducing the new bPod**  
Peter

This is a day I've been looking forward to for 15 years. Every once in a while a revolutionary conference badge comes along that changes everything. And BSides Canberra has been fortunate to deliver a few of these into the world. In this talk I will be introducing 3 new products in this class - a colour screen badge with touch controls, a revolutionary hardware learning device and the 3rd is a breakthrough hacking and CTF challenge...

Main Track

Royal Theatre

10:30 AM

### 10:30 AM Designing a Badge Add-on in KiCad Day 2

AM Josh Johnson

2h Ever wanted to design a PCB but unsure where to begin? This workshop will be a guided tour through designing a badge add-on in KiCad, concluding in assembly of the add-on which you can proudly attach to your conference badge to show off your newly acquired skills. Please bring a laptop with KiCad installed and a mouse to get the most out of the workshop.

Event Track

Hardware Village Stage

11:00 AM

### 11:00 AM Scudo Allocator exploitation

AM Zac Ecob

55min The Scudo allocator is a memory allocator designed primarily for C/C++. Designed as part of the LLVM project, it has gained popularity as an alternative choice to allocators like ptmalloc2, most prominently being used as Android's default allocator since Android 11. Scudo aims to provide efficient memory allocation and deallocation whilst mitigating common vulnerabilities such as heap buffer overflows, use-after-frees, and double frees. As the risk associated with these vulnerabilities continues to rise, scudo is primed to become more and more of a prominent choice for developers to use....

Main Track

Royal Theatre

12:00 PM

### 12:00 PM Going out on a Limb: Accelerating Elliptic Curve Cryptography

PM Rohan McLure

25min Cryptographic libraries such as OpenSSL and GNU Nettle form the backbone of security in the current day. Proving authenticity online, establishing secure communication channels etc all depend on complex mathematical structures, including algebraic groups on Elliptic Curves.

Main Track

Royal Theatre

1:30 PM

### 1:30 PM Bringing Harmony to IIS: Using game mods to protect (or nuke) your web server

PM Adrian Justice

55min With an ever increasing number of developers using .NET based game engines, game modders have developed sophisticated tools which can interact with the .NET Common Language Runtime to modify game mechanics, add features and fundamentally modify how games operate at runtime.

Main Track

Royal Theatre

2:30 PM

### 2:30 PM GetInjectedThreadEx - improved heuristics for suspicious thread creations

PM John Uhlmann

55min Since its debut in 2017, Get-InjectedThread.ps1 has been a blue team staple for identifying suspicious threads via their start addresses. However, red teams have subsequently identified low-cost evasion techniques to counteract this - obfuscating their shellcode threads with start addresses within legitimate modules.

Main Track

Royal Theatre

3:00 PM

### 3:00 PM RF Demos

PM Amy Nightingale, John Gerardos

20min Radios are everywhere, and RF technology is applied in places that you might not even have thought of, and this usage is only going to grow. Come learn how basic Radio technology works, what you can transmit and receive, as well as the legalities you need to keep in mind before blasting the entire CBD with RF interference (hint: don't).

Event Track

Hardware Village Stage

4:00 PM

### 4:00 PM An abridged history of Linux kernel hardening

PM Russell Currey

55min The Linux kernel is everywhere. It's running on billions of devices here on Earth, and quite a few in space, too. Linux is big and complex: it does a lot of stuff, it runs on a lot of things, it's deployed in a lot of ways, and it has many distributions with many versions, each with their own modifications.

Main Track

Royal Theatre

5:00 PM

### 5:00 PM The Dark Side of Large Language Models: Uncovering and Overcoming of Vulnerabilities

PM Javan Rasokat

25min As the use of AI in cybersecurity continues to grow, many researchers have looked to large language models (LLMs) to help identify vulnerabilities in code. However, recent studies have shown that LLMs may not be as effective as initially thought, and can even introduce new vulnerabilities into code. This talk will explore the potential risks and challenges associated with using LLMs for vulnerability detection, including the potential for introducing new vulnerabilities into code....

Main Track

Royal Theatre

6:30 PM

### 6:30 PM Official BSides Canberra Party

5h The BSides Canberra Official Party is back for 2023. It will be a foodies heaven with food to purchase and a sizeable bar tab. Join us to celebrate on Friday night. More details on the location will be given at the conference.

Event Track

Logistics

Saturday 30. September

9:00 AM

### 9:00 AM Black Bag

AM Ty Ridgeway, Julian Abrahams, Redacted

6h A black bag is a physical security competition where teams of participants attempt to capture intelligence (flags) from a physical environment without being detected.

Registration can be done here: <https://blackbag.redacted.au/>

Event Track

Blackbag Room

**9:00 AM** CTF Mayhem Unleashed!  
Cybears  
6h  
The Cybears will return to run the BSidesCBR 2023 Capture-The-Flag competition! A CTF is a competition where teams use their knowledge of computer and network security to solve challenges in a Jeopardy format. The challenges may cover topics such as web exploitation, binary exploitation, cryptography, reverse engineering and will include challenges for people just getting started in the industry as well as seasoned CTF players....  
[Event Track](#)  
Competition Room Stage 1

**9:00 AM** HuntIR by ACSC  
ACSC  
6h  
Do you want to try out your incident response skills for a day? Want to know what it is like to perform technical analysis when the pressure is on? Come and try the Australian Cyber Security Centre's Incident response game – HuntIR. HuntIR is an incident response game developed by the Digital Forensics Incident Response team that focuses on the analysis of technical artefacts to answer key investigation questions. Each player is given 24 hours to perform technical analysis on their own unique incident that includes various logs including process listings, autoruns, IIS access logs and more. Stay in regular contact with your victim organisation ...  
[Event Track](#)  
Competition Room Stage 2

9:05 AM

**9:05 AM** Keynote Session: The Journey to Mastery  
Louis Nyffenegger  
55min  
Join Louis, who has spent a decade guiding others through PentesterLab, as he helps us delve into the journey from beginner to mastery. This talk will outline this exhilarating journey, providing practical advice on how to seamlessly transition from one learning stage to the next. We will also tackle the common challenges and setbacks most individuals encounter on this learning path.  
...  
[Main Track](#)  
Royal Theatre

9:30 AM

**9:30 AM** Hardware & Wireless Village  
7h  
Bored with tcpdump? IDA got you down? Forget your neglected VMs, come hack hardware! Bring your RTL-SDR dongles, buspirates, and '80s phone phreaking kit - let's hack together!  
Soldering irons will be available for all you tech wizards. You can use them to make badge modifications or for any other hardware hacks you have in mind. Need help with your conference badge? We've got your bac...  
[Event Track](#)  
Hardware & Wireless Village

**9:30 AM** Locksport Village  
7h  
Get ready to immerse yourself in the captivating world of locksport. Our doors swing open each day from 10 am to 5 pm, welcoming all curious souls. Locks, tools, and seasoned instructors are at your disposal, so why not seize this golden opportunity to learn a trick or two from the experts?  
...  
[Event Track](#)  
Locksport

10:00 AM

**10:00 AM** RF Demos  
Amy Nightingale, John Gerardos  
20min  
Radios are everywhere, and RF technology is applied in places that you might not even have thought of, and this usage is only going to grow. Come learn how basic Radio technology works, what you can transmit and receive, as well as the legalities you need to keep in mind before blasting the entire CBD with RF interference (hint: don't).  
...  
[Event Track](#)  
Hardware Village Stage

**10:00 AM** Hardware in the Loop: Building a Rack for Substation Protection  
Courtney  
25min  
The changing way our operational technology environments are connected and operated exposes our critical infrastructure to more cyber security threats than ever before. This presentation will discuss the Rack for Substation Protection, a new physical system recently purchased to enable research and training of protection relays, a critical component of electrical substations.  
[Main Track](#)  
Royal Theatre

10:30 AM

**10:30 AM** Designing a Badge Add-on in KiCad Day 3  
Josh Johnson  
2h  
Ever wanted to design a PCB but unsure where to begin? This workshop will be a guided tour through designing a badge add-on in KiCad, concluding in assembly of the add-on which you can proudly attach to your conference badge to show off your newly acquired skills. Please bring a laptop with KiCad installed and a mouse to get the most out of the workshop.  
[Event Track](#)  
Hardware Village Stage

11:00 AM

**11:00 AM** AFK  
AFK Choir  
20min  
Escaping from both computer and piano keyboards, the singers of AFK are here to entertain with music inspired by classics of geek culture including Star Wars, Star Trek, zombies, computer games, and Lord of the Rings, along with the ought-to-be-classics by Jonathan Coulton and Miracle of Sound.  
...  
[Main Track](#)  
Royal Theatre

11:30 AM

**11:30 AM** Don't Lookaside or you'll miss it: Turning a Hyper-V cache miss into 200k cash  
Leo Adrien  
55min  
Hyper-V has long been considered a prestige target for security researchers, with Microsoft offering high value bug bounties, and performing continuous in-house testing and attack-surface hardening. In this presentation I'll show how I turned the discovery of a seemingly unreproducible bug into a critical-rated arbitrary code execution vulnerability, which was awarded MSRC's maximum bounty.  
...  
[Main Track](#)  
Royal Theatre

1:30 PM

**1:30 PM** IoT Malware IRL  
David Collett  
55min  
David will present some new IoT malware he discovered, by accident, on a wifi photo frame purchased at a physical store right here in Canberra. He will describe the tools and techniques used to locate and extract the...  
[Main Track](#)  
Royal Theatre

2:30 PM

**2:30** Modern Linux Kernel Mitigations

PM  
55min  
Ray Veldkamp, Matt Kurz

The Linux kernel has long been an attractive target for attackers aiming to compromise systems, as a result the kernel community are constantly responding by introducing security mitigations and locking down attack surfaces. Linux distributions will often weigh up the impact of enabling these features, with the impact to usability and performance of the operating system, resulting in a fragmented approach to adoption of upstream Linux kernel security features. This talk will discuss a range of recently introduced security features in the kernel, which attempt to complicate the exploit development process, and provide an overview of t...

Main Track

Royal Theatre

3:00 PM

3:00 PM  
20min  
RF Demos  
Amy Nightingale, John Gerardos

Radios are everywhere, and RF technology is applied in places that you might not even have thought of, and this usage is only going to grow. Come learn how basic Radio technology works, what you can transmit and receive, as well as the legalities you need to keep in mind before blasting the entire CBD with RF interference (hint: don't).

...

Event Track

Hardware Village Stage

4:00 PM

4:00 PM  
25min  
Fan-Tastic RFID Thief: Revamping an old weaponised RFID reader tool  
phish

The Tastic RFID Thief was first presented by Francis Brown from Bishop Fox at Defcon back in 2013. Since then, long-range RFID readers have been used by many red teamers to successfully capture employee access card credentials. 10 years later, this tool still plays a crucial part in many engagements where insecure RFID cards are used. However, there have been few improvements to the tool despite the advances in cheap microcontrollers and battery technology. It's time to give this tool a breath of fresh air and make it Fan-Tastic.

Main Track

Royal Theatre

4:30 PM

4:30 PM  
55min  
Closing Ceremony

Join us at the closing ceremony, where we will announce the winners of the competitions and reflect on the valuable moments from this remarkable conference. It's a great opportunity to appreciate the connections and networking that have blossomed during these inspiring days. We extend our heartfelt gratitude to our supporters, speakers, sponsors, and volunteers for their invaluable contributions. We look forward to seeing you there as we bid a fond farewell and embrace the exciting journey ahead!

Main Track

Royal Theatre