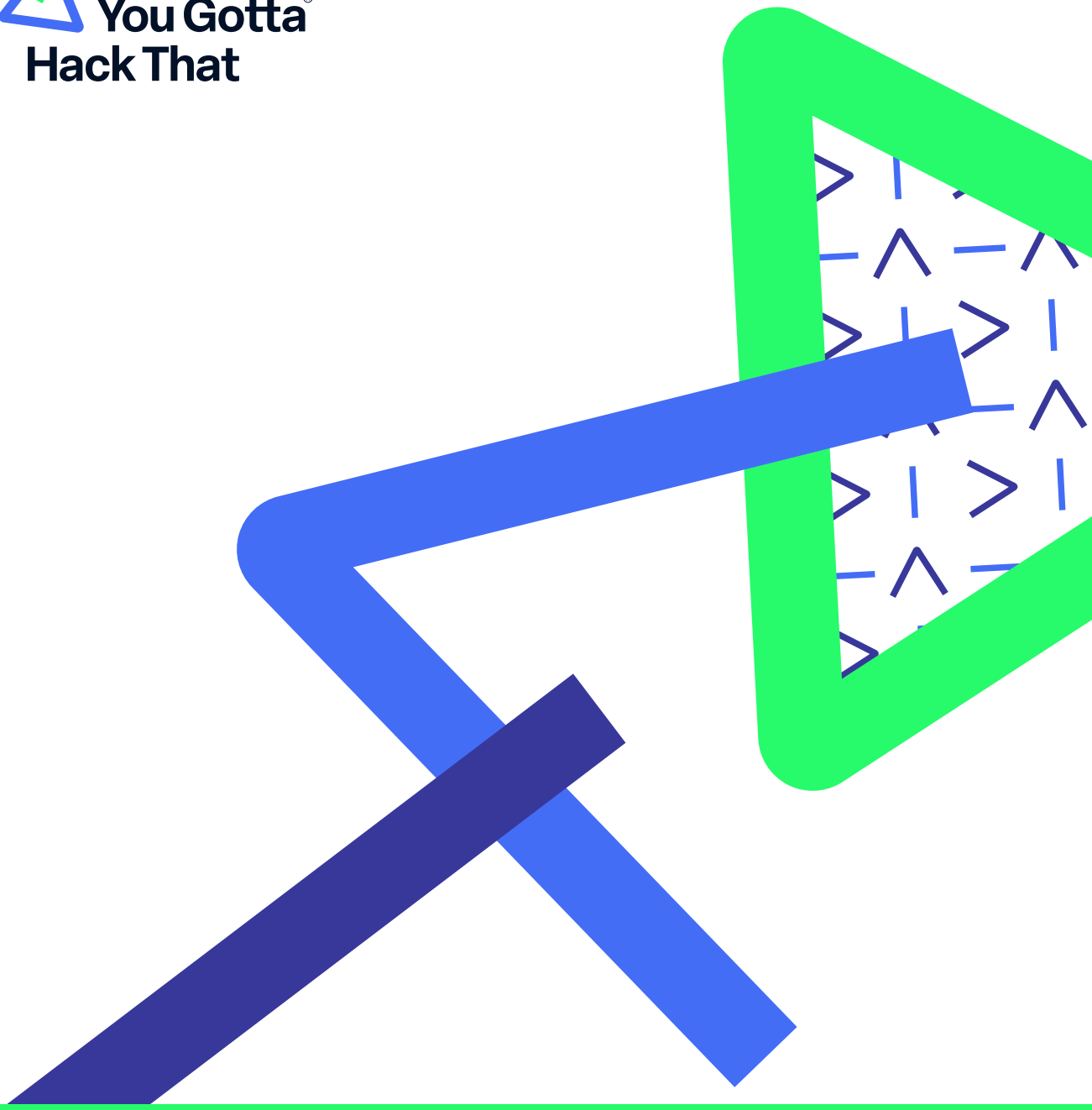
OT and IoT Penetration Testing and Hacking Training

To illuminate your weaknesses and empower your people

You Gotta® Hack That



Email us: helpme@yg.ht **Call us:** +44 161 398 0703 **Visit:** yougottahackthat.com

Contents

We offer specialist penetration testing and hands-on hacker training to safeguard your technology and elevate your team's capabilities. The security of IoT and OT systems has never been more crucial, so dive into our comprehensive services and discover how we can help you stay one step ahead of your cyber threats.

Who is You Gotta Hack That®?

You Gotta Hack That® is a boutique cyber security consultancy specialising in embedded systems and the Internet of Things. We're highly trained and experienced in this particular penetration testing niche, and combine that with our strong analytical and consultancy skills to give you ultimate peace of mind.

Felix

FOUNDER & PRINCIPAL HACKER

Felix is a geek through and through. He self-taught BASIC programming as a child and has experience in many different programming languages and areas of technology. He had a non-standard academic education which resulted in getting a distinction at Masters level from the University of Oxford but never actually getting a bachelor's degree. He got into trouble at school for breaking into computers and hasn't stopped since. Felix focuses on all things reverse engineering and loves to find vulnerabilities in the firmware he has extracted from a new device.

Pete

WEB APPLICATION & CODE ANALYSIS EXPERT

Pete is a relentless innovator in web and thick-client technologies. With deep expertise as both a developer and hacker, he's known for creating custom tools and delivering exceptional results. Always eager to share his knowledge, Pete constantly pushes the limits, surprising clients and colleagues alike with his dedication and ingenuity.

Charles

INFRASTRUCTURE PENETRATION TESTING SPECIALIST

Charles thrives on the challenge of outmanoeuvring defences to achieve his objectives. With extensive experience across diverse, high-profile organisations, he excels at assessing technical vulnerabilities and contextualising risks for clients. A lifelong learner, Charles continually expands his expertise, staying ahead of emerging threats. His impressive array of security certifications is a testament to his dedication and passion for the field.

Rob

RESEARCH & REVERSE ENGINEERING SPECIALIST

Rob is a master of researching unusual problems and loves nothing more than working on an innovative attack strategy. He is noted for his passion for software reverse engineering and skills at building electronics. His enthusiasm is infectious and he brings a welcome hands-on approach to problem-solving. Even in his spare time, he's always pondering the seed of a new idea, so you can often find him soldering and crafting new tech.

Chris

PROGRAMMING & DIGITAL FORENSICS EXPERT

Chris brings extensive experience in C/C++ and C# programming, coupled with deep expertise in digital forensics. His forensic skills span a wide range of devices, from traditional computers and mobile devices to embedded systems and IoT gadgets. Known for his calm and methodical approach, Chris excels at analysing complex problems across diverse platforms. He is always eager to share his knowledge and engage in discussions, making him a valuable mentor and collaborator for those passionate about technology.

How are we different?

Consultant-led

Our consultants love what they do. They love it because they do things that are enjoyable, mentally challenging and because they can do the right job for the customer. This sense of job satisfaction is achieved because the consultants aren't constrained to a checklist approach or an overly structured job sheet. For the customer, this is important, not only because a happy consultant is a good consultant, but because they will be able to give you what you need.

Great expertise

A wise business person once told Felix that the people in any given business are crucial and make an enormous difference to its ability to succeed. **Everyone at You Gotta Hack That® is chosen for their enthusiasm, their wealth of experience and strong capabilities.** These qualities mean that when you select You Gotta Hack That®, you get to take advantage of our world-class expertise.

Agility

We are a collective of individuals who quickly and concisely make progress on the things that matter the most. We recognise when change is required and make it happen.

As we aren't a mammoth organisation, we don't have the layers of management and bureaucracy that slow down decision making and constrain people into treading the well-trodden path.

This level of agility can only be a good thing for our customers because it means we are always at the bleeding edge of what we do, and we can respond to our customer's needs without fuss.

Actively involved in the hacker community

Just because someone has a job as a penetration tester, it doesn't make them a hacker.

The term hacker is wildly misunderstood by the general public, as it tends to bring to mind stereotypes such as the antisocial, hoodie-wearing teenager skulking around late at night. The hacker community was spawned by technology geeks whose hobby was fiddling with electronics to make them better or simply to understand how they worked.

At You Gotta Hack That®, we know that the best penetration testers are also guided by this same hacker mentality. That is why they all actively engage with the 21st century's Hacker community. We each get involved in many ways, including attending and speaking at conferences, co-authoring books, publishing tools, writing blog posts, and performing research. Being firmly embedded in the hacker community is an advantage for our customers. It means the consultants are well-versed in the latest tools and techniques as well as having had their hacking mentality continually strengthened.

No sales axe to grind

We are proudly not interested in sales tactics, hard sells, upselling opportunities, or any other technique to extract money from our customers. Instead, we rely on you to recognise that we provide our services for the right reasons, that we are good quality, and that we are appropriately priced.

Passionate about what we do

Each of us arrived at this point in our lives because we utterly love what we do. In our opinion, **there is no more incredible a thrill than getting past the security of a system and helping our customers make improvements.**

For us, hacking isn't a job; it is a devotion. Some people go further and call it an obsession. It's these reasons that mean when you choose You Gotta Hack That®, you get people who push boundaries and explore the details. All this passion provides you with the security assurance you want and desire.

No pretence: you get what you see

Each of us has the quality of being understated and straightforward. Life like this is incredibly simple because we know that there is no bluster or over-promising. We believe our customers recognise this quality in us and see that it makes us easily blend into their team when we are working together.

Always close to the action

Each of us is actively involved in improving our skillsets all the time. **All forms of penetration testing move at breakneck speed, and if we aren't continually learning, we are falling behind.** On the surface of it, that sounds like lots of pressure, and it probably is. However, this is what we do because we love it.

If you look hard enough, you will always find us exploring cybersecurity. That could be writing code, studying a new exploit, reading technical specifications, or attending a course. Ask any of us what geeky thing we have been doing recently, and you are likely to get more information than you bargained for!

Qualified

Between the team we have a wide variety of certifications, qualification, and training courses. To name a few we have: Crest Certified Practioner Security Analyst (CPSA), Crest Registered Tester (CRT), Crest Certified (Infrastructure) Tester (CCT Inf), PenTest+ Beta Testers by CompTIA, Offensive Security Certified Expert, Offensive Security Certified Professional, Offensive Security Wireless Professional, GIAC Penetration Tester, Certificate in Information Security Management Principles by The British Computer Society (BCS), Amazon Web Services Cloud Practitioner, Bachelors and Masters Degrees, ARM IoT Firmware Exploit Lab, Trainer for the Foundations of IoT Security, Red Teaming Bootcamp by Nettitude, Advanced Infrastructure Hacking 2 (AIH2) by NotSoSecure, Certified Information Systems Security Professional (CISSP) by ISC(2), Red Team Operations by SpectreOps.

IoT and OT Penetration Testing Services

What is Operation Technology and IoT penetration testing?

Penetration testing is the art (and science) of hacking into a computer system to exploit cyber security vulnerabilities. This is done to show the developers, owners or operators of the system any vulnerabilities that are present, so that they can understand the level of risk and choose whether to take corrective action.

Unlike standard IT environments, OT and IoT systems require specialised testing methods to account for their complexity, real-time operations, and the critical nature of their functions. Penetration testing ensures that even the most intricate and unconventional vulnerabilities are brought to the foreground.

What challenges are there for OT and IoT penetration testing, and how do we deal with them?

Embedded systems such as IoT devices and those in OT environments have additional attack surfaces compared to traditional IT systems. This requires specialised penetration testing, which everyone at You Gotta Hack That® is highly trained in.

In addition, real threat actors often take months or years to evade security systems in IoT and OT environments, which means the condensed timeframe of penetration testing can feel artificial. By keeping you as an integral part of the decision-making process, we ensure that we can do as much as possible for your specific system, and that you understand any possible constraints.

Who needs IoT and OT penetration testing?

- Organisations that create or provide IoT, OT or embedded systems
- Organisations that use IoT or Operation Technology on a large scale or for mission critical purposes
- Organisations that are obligated by law (e.g. the 2022 PSTI Act in the UK).
- Organisations with standards compliance requirements, or mandated assurance requirements within client contracts (such as the need for ISA 62443 adherence).

The most mature cyber security is usually found where penetration testing is embraced, because they know it is the right thing to do for everyone!

What you get

Detailed Reports: covering the vulnerabilities found, their potential impact on the system itself, and suggested options for corrective action.

Actionable Insights for All Stakeholders: crafted to be accessible to both technical teams and business leaders, ensuring that all stakeholders understand the risks and the necessary steps to mitigate them.

Thorough Debriefing Session: so that relevant questions can be dealt with immediately, or discussed where there is nuance and complexity.

Continued Support: before, during and after your penetration testing exercise, to ensure your security staff understand how the findings affect your systems and can implement the solutions.

Retesting: after your corrective action, to confirm that the identified vulnerabilities have been effectively addressed.

01> Hardware Hacking

Ensuring your physical devices aren't the weak link in your security chain.

Hardware hacking and reverse engineering assesses the security of physical devices used in both Operational Technology (OT) and Internet of Things (IoT) systems. By dissecting the hardware, we uncover vulnerabilities that could be exploited by attackers, whether the device is part of a critical OT environment like a manufacturing plant, or an IoT device used in a domestic smart refrigerator.

There is a staggering number of IoT and embedded devices in the world, each presenting their own set of risks. Each of these devices is essentially a mini-computer, but unlike traditional IT systems such as web applications, these miniature computers are physically in the hands of potential attackers. Their physical accessibility, combined with the fact that they often hold sensitive data and control critical operations, makes them prime targets for attackers. Compromising a single device can lead to significant operational disruptions, safety risks, or even widespread cyber-physical attacks across the rest of the environment. This service helps you understand how advanced an attacker needs to be to breach your devices, so that you can take proactive measures to strengthen your defences.

Our combination of testing techniques includes extracting and examining the firmware, analysing circuit boards, and identifying potential points of compromise. Exercises such as these can require specialist equipment and is often destructive in nature.

As devices can vary hugely, all aspects of our Hardware Reverse Engineering is made-to-measure. Throughout the process, we work closely with your team to ensure that the testing aligns with the device's technical needs, your security objectives, and your operational needs.

Who?
Any company that uses, develops, owns, or operates embedded devices such as IoT or OT

What?
Hardware reverse engineering and exploit development against the device

Why?
To understand how advanced an attacker needs to be before they can breach the device and enable appropriate defences to be designed and implemented

How?
Remote consultants using destructive and non-destructive testing techniques against the end-device

Who?
Any company that uses, develops, owns, or operates IoT or other embedded systems

What?
Firmware reverse engineering, vulnerability discovery, and exploit development

Why?
To develop an understanding of how advanced an attacker needs to be before they can breach the device

How?
Remote consultants using software reverse engineering techniques against the firmware

02> Firmware Hacking

Deconstructing firmware to identify vulnerabilities.

Firmware hacking and reverse engineering analyses the software embedded within your OT and IoT devices. Firmware provides the core functionality of these devices, and often has a large attack surface area. This service involves acquiring, reverse engineering, and examining the firmware to identify vulnerabilities that could be exploited by attackers. Optionally, exploits can then be developed to demonstrate tangible impact as well as to further examine the deeper levels of attack surface.

Embedded devices are used in a broad range of physical contexts, meaning that attackers are much more able to perform physical attacks. Traditional IT systems often rely upon security controls that can't fully cater to the nature of an embedded device. Vulnerabilities in firmware can lead to serious consequences, such as unauthorised access, data breaches, or even complete device or ecosystem takeover. In OT environments, such breaches can cause operational downtime or safety hazards, while in IoT systems, they can lead to significant privacy concerns, reputational loss, financial penalties and even danger to life. Firmware reverse engineering provides actionable intelligence and helps you quantify risks and implement appropriate safeguards.

Firmware is acquired either directly following a hardware reverse engineering exercise or by using provided firmware files. Once extracted, we deconstruct the firmware to understand its architecture, functionalities, and potential weaknesses. This process includes vulnerability discovery, code analysis, and where appropriate, exploit development to assess how vulnerabilities could be leveraged by an attacker. Our experts use advanced tools and techniques to achieve a deep understanding of the firmware's security posture.

03> Wireless Networks and Radio Frequency Communication Hacking

Testing within radio range of the target system.

Wireless and RF communications are crucial for OT and IoT systems, facilitating remote control, data exchange, and device interaction. Unlike traditional penetration tests that focus solely on WiFi, we assess a range of wireless and RF communications, including Bluetooth, ZigBee, LoRaWAN, and NFC.

By evaluating these communications, we help ensure your OT and IoT devices are secure against wireless-based attacks that could compromise functionality or data integrity. RF-based threats like interception, jamming, and spoofing, as well as digital vulnerabilities such as hardcoded NFC credentials or unencrypted LoRaWAN functions, are key areas of focus.

The range of wireless technologies directly impacts the likelihood and ease of exploitation by attackers. Longer ranges may attract more attackers due to reduced risk. We identify wireless and RF risks, enabling you to implement necessary protections.

Our experts assess encryption, authentication, and access control mechanisms whilst within radio range of the target system. Testing is typically done in a controlled environment to minimise disruption and ensure accurate results. If this isn't feasible, we collaborate with you to find an alternative.

Our process begins with a survey of the wireless and RF protocols in use, followed by deploying equipment for protocol fuzzing or tailored attacks specific to the identified protocols.

Who?
Any organisation that uses or develops devices that have a wireless networking or RF communications interface

What?
Wireless network penetration testing against the protocols in use

Why?
To expose weaknesses in wireless communications that adversely affect OT and IoT devices

How?
On-site or remote consultants using specialist equipment to attack RF communications and wireless networks

"Working with You Gotta Hack That® has enabled us to demystify the hype and fear mongering that surrounds cyber security, prioritise our technical and regulatory roadmap and develop a clear cyber strategy. Having expert external support has enabled us to expand our teams knowledge whilst also freeing up their time to focus on building an awesome product, knowing that we can call on the relevant expertise whenever required."

Mike Tinmouth, Chief Operating Officer @ AQUA Ocean

Case Study A

Introduction

As a leader in drone ship design and manufacturing, we recognised the need to ensure our cyber security was up to the necessary technical, regulatory and commercial standards. We sought expert support through advisory services and assurance activities, including penetration testing, to achieve this goal.

Solution

We partnered with a specialist firm to help us navigate the cyber security challenges of our novel drone ship project. Together, we discussed the ship's hardware and software design, its components, and our specific security objectives and challenges. From these discussions, a series of focus areas were established, each with corresponding activities. The majority of these activities were educational, aimed at enhancing the cyber security knowledge and self-sufficiency of our design and engineering teams. Additionally, a series of targeted and comprehensive penetration tests were conducted to assess our security posture.

Results

The collaboration proved to be highly beneficial. Early identification of potential issues allowed us to make crucial adjustments to our design and architecture, significantly improving our cyber security maturity. This proactive approach not only strengthened our security but also saved us valuable time and resources by reducing future cost and complexity. Moreover, the engagement provided us with a defined roadmap for future security enhancements and milestones.

Conclusion

We have built a strong relationship with our cyber security partner and continue working together on ongoing iterations and development. Their expertise continues to be invaluable as we develop and refine our projects, ensuring that our approach to cyber security remains not only robust and resilient but also industry leading.

Who?
Organisations that design or operate OT or IoT ecosystems that include a web app, mobile app, or API

What?
A web application, mobile app, or API test of the web-based system

Why?
To understand what a malicious user of each web application or API can achieve

How?
Consultants working against selected web components using modern tools and tactics

04>
Web Application Penetration Test

Attempting to break into a specific web application.

Web applications, mobile apps and web APIs play a significant role in today's interconnected environments, often serving as the interface for managing PLCs, network gateways, controlling the device during normal operation, and presenting data that may be confidential or personal. The test is influenced by the attack surface. This includes how it's hosted, the wider system that the web app inhabits, the potential for risk profiles that may have much greater impacts but much lower likelihoods, and more.

Web-based services are often poorly secured, with the potential to be more exposed than other parts of these systems. As such the attack methodologies are relatively widespread and well-understood. Combined with the cyber-physical effects that can be achieved with their abuse – such as data manipulation, service outages, or even physical harm - they are a primary concern for many IoT and OT operators.

Penetration testing identifies vulnerabilities such as insecure data transmission, authentication flaws, and misconfiguration. Discovering these issues before attackers exploit them gives you a fighting chance to successfully defend your systems.

With cloud-based systems we perform our testing over the Internet. For device-hosted targets we prefer to take a representative system back to our lab for testing, as this gives us a better opportunity to complete any required research and development, though we are also happy to work on site if this is needed. No matter the target, our team always pays attention to the details.

05> Infrastructure Penetration Test

Assessing the security of the infrastructure supporting your IoT and OT environments

Modern systems are found with many diverse architectures, including traditional on-premises systems, cloud-hosted environments, and hybrid models. Our testing is comprehensive and covers components such as network backbones, End User Devices (EUD), management devices, perimeter defences, and remote access systems, regardless of where they are hosted. Whether it's the servers running your industrial control systems or the cloud platforms hosting your IoT data, we simulate the threats you are most concerned about.

Infrastructure forms the base layer of your entire operation, meaning that the infrastructure underpinning key operations are particularly potent entry points for attackers. The shift towards cloud-based solutions also introduces new security challenges that traditional testing methods might overlook. The impacts of a breach here could include disruption to the organisation, sensitive data being compromised, or endangering safety. Our service ensures that every part of your infrastructure is analysed, so that you are armed with the knowledge crucial to protecting both your operational integrity and your organisation's reputation.

We utilise our expertise to ensure that the most sensitive components are prioritised across your network architecture, firewall configurations, remote access points, and many other internal systems. For cloud environments, we assess the configuration of your cloud accounts. As our approach is tailored to your specific needs, our efforts might then be targeted on identity and access control mechanisms, data storage practices, cloud-based network access controls, CI/CD pipelines and the security of any integrated services.

Who?
Any company that uses, develops, owns, or operates IoT or Operational Technology

What?
An infrastructure and cloud penetration test of some or all of your infrastructure

Why?
To assess what damage an attacker can achieve when they breach the perimeter and gain a foothold at a low level within your environment

How?
Consultants attacking over the Internet, on-site, or with our bespoke remote access solution, the SmuggleBox

“Felix and the team supported us through a very difficult time. We knew we had security issues but had no idea about how to find and deal with them. Their guidance and expert analysis lightened the load considerably!”

Adrian @ Client B

Case Study B

Introduction

A client specialising in high-end Internet-of-Things (IoT) devices for home use was approached by a cybersecurity researcher who identified severe flaws in their systems. The researcher requested corrections within 90 days before publishing the findings. With a small technology team lacking cybersecurity expertise, the client sought help from You Gotta Hack That® halfway through the disclosure period.

Solution

You Gotta Hack That® assisted the client both on the business and technical fronts. They helped the client understand Responsible Disclosure and guided their response. Technically, You Gotta Hack That® conducted a full product assessment and validated corrective actions, including re-writing cryptography routines and improving credential handling.

Results

With You Gotta Hack That®'s support, the client successfully published major fixes before the 90-day Responsible Disclosure period ended. The critical flaws were resolved, leading to improved security across their IoT devices, including enhanced cryptography and more secure credential management.

Conclusion

This anonymised case study demonstrates how You Gotta Hack That® quickly and effectively assisted a client lacking cybersecurity expertise, ensuring that their IoT products remained secure and that the researcher's findings were addressed in a timely manner. At You Gotta Hack That®, client privacy is a top priority. All projects are assigned code names, and client identities are never disclosed without permission.

What happens after a test?

We start with an in-depth debrief where we go through as much or as little detail as you need. These are often an hour or two long and can comprise of one or more groups of people such as a management review and a technical review.

What happens next for you depends largely on the outcome of any test undertaken. We will discuss this with your during the debrief.

In the following two weeks, we will happily help with further technical enquiries via email for free. After which we may need to charge, for example, if the support takes a large amount of time.

As part of the scoping and debrief calls, we will discuss retesting. Retesting is where we check that the corrective actions you have put in place have successfully dealt with the security problem. Retesting needs to happen within three months of the end of the penetration test and can be between 1 and 5 days, depending on the size of the original test.

Not sure what you need?

We can help!

There's a saying in the industry - **it's not if you will get hacked, it's when**. Contact us and our consultants will be happy to help you get your geek on.

Email: helpme@yg.ht
Call: +44 161 398 0703
Visit: yougottahackthat.com
Listen: /podcast

The Certified Embedded System Hacker Training Course

First two modules available now, with new modules coming soon.

Despite the increasing importance of IoT and OT cybersecurity, there aren't many ways for individuals to break into this interesting niche of the penetration testing industry. That's why we've created this certified course, designed as a holistic approach to penetration testing for embedded systems such as Internet of Things devices and Operational Technology environments.

Each module demystifies the secrets of one area of IoT, OT, and embedded system penetration testing. Individual modules can be taken as one off, stand-alone training, or combined to gather knowledge and skills that work in harmony.

Designed for current penetration testers and technical professionals, these modules tend to be complex and intense – so if you work in IoT or OT cyber security, or are a penetration tester wanting to further specialise, join us for a deep dive into the intricate world of embedded systems hacking.

The Certified Embedded System Hacker Training Course

Course highlights

The overall course is comprehensive, helping you gain expertise across a wide range of topics including:

- Foundational embedded system knowledge
- Electronics and PCB reverse engineering
- Firmware extraction
- RF hacking (Bluetooth, ZigBee, NFC)
- ...and more

You'll cover advanced subjects exclusive to this course as an unparalleled singular collection of knowledge and skills, with depth in each subject beyond that which is readily available elsewhere.

Unlike typical capture-the-flag sessions, this course is delivered via intensive, immersive, instructor-led training. We provide real-world skills essential for hacking IoT and OT environments in a manner that suits many learning styles. The courses are intense, but should never leave you with unanswered questions or unhelpful leaps of faith that will continue to hinder your expertise.

We take a limited number of students onto each module to ensure everyone gets the attention they deserve, and offer a mix of onsite, online, and hybrid modules to suit your learning style and budget.

Who should attend?

This course is ideal for technical professionals with a passion for cybersecurity, regardless of certifications or years of experience. All you need is enthusiasm, technical aptitude, and the readiness to tackle challenging, hands-on training.

We welcome those who identify as neurodivergent, and have designed the course with a diversity of learning styles in mind.

Certification

Upon completion, participants will receive certification for module attendance. Each module also contains an optional certification process, displaying that individual's expertise in both the module and the cutting-edge field of embedded system penetration testing.

Course modules available at launch

- Electronics and PCB reverse engineering
- C programming for embedded systems

This course is new and we need beta testers. Sign up to be a beta tester to get £1000 off the standard price.

Course modules coming soon

- Foundational embedded system knowledge
- Firmware extraction mastery
- Firmware emulation and peripheral fakery
- Software Reverse Engineering (SRE)
- Firmware Reverse Engineering (FRE)
- RF hacking: Bluetooth, ZigBee and NFC
- RF hacking: the unusual, the weird and the wonderful
- Hacking the embedded ecosystem
- Digital forensics on ubiquitous tech
- Glitching and power analysis

If you want a particular module to be released soon, get in touch to find out its launch date.

Electronics and PCB Reverse Engineering - 5 days, in person

This module offers an in-depth exploration of Printed Circuit Boards (PCBs) and electronic components, designed for those looking to deepen their understanding of hardware at a cybersecurity level. Participants will learn to analyse unfamiliar PCBs, identify attack surfaces, and perform tasks such as firmware extraction. The course blends theory with hands-on practice, covering PCB design fundamentals and advanced techniques like glitching and power analysis.

Students will master reverse engineering, understand inter-component communication, and use essential lab equipment. Key practical skills like soldering and using multimeters and logic analysers are also covered. You'll gain the knowledge and skills to tackle hardware reverse engineering and identify security issues.

Packed with exercises that bring theory to life, this module is an exciting journey into embedded system hacking. Join us to confidently address cybersecurity vulnerabilities in hardware and take your skills to the next level.

C programming for Embedded Systems - 5 days, in person

This module bridges the gap between cybersecurity and embedded systems programming, equipping you with the skills to analyse and write code for target devices. Designed for skilled programmers with limited experience in C or C++ on resource-constrained devices like IoT or OT systems, the course explores the challenges of low-level programming with a hacker's mindset.

You'll learn cross-compilation, memory management, and address-based peripheral access while addressing resource constraints and security implications. The module balances theory with hands-on exercises, covering core concepts such as loops, pointers, and Object-Oriented Programming (OOP). You'll also dive into network communications, low-level hardware interaction, memory mapping, bare-metal programming, and error-handling in the physical world.

Uniquely, this course doesn't teach you to hack poorly written code—it teaches you to write it, highlighting security pitfalls and programming possibilities in embedded environments. By the end, you'll have a strong foundation in embedded C and C++ programming with a cybersecurity focus, ready to tackle real-world embedded systems challenges.

Upgrade your programming skills and master embedded systems! Dive deep, code smart, and become an expert in building and breaking devices. Enrol today to start your journey.

Enrol now and take the first step toward mastering embedded system hacking with our cutting-edge Certified Embedded System Hacker Training course.

Email: helpme@yg.ht Call: +44 161 398 0703 Visit: yougottahackthat.com

Internet of Things and Operational Technology cyber security confidence starts here.

Contact You Gotta Hack That® today to discuss your offensive cyber security training and penetration testing needs.

Email
helpme@yg.ht

Call
+44 161 398 0703

Visit
yougottahackthat.com

Listen
/podcast