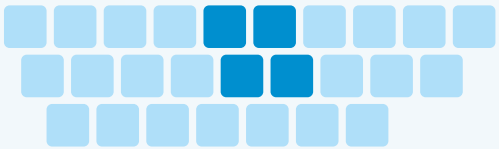
You Gotta Hack That



Cyber Threat Simulation and Penetration Testing

Email us: helpme@yg.ht **Call us:** +44 161 818 9448 **Visit:** yougottahackthat.com

CONTENTS

Printed on 100% recycled paper.

WHO IS YOU GOTTA HACK THAT?

You Gotta Hack That is a boutique cybersecurity consultancy that specialises in cyber threat simulation. Those familiar with the industry will think of our work as penetration testing, but, we think of it as more than just that. We know this belief is true because we don't just test the security of systems; we use our expert knowledge to emulate real threat actors. We thrive on our ability to help our customers improve their level of cybersecurity protection. We achieve this every time we discover a flaw and then provide education to our customer's staff about its security implications.

Felix

FOUNDER AND 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. Despite a non-standard early education, he achieved a distinction at Masters level in Software and Systems Security at the University of Oxford. He got into trouble at school for breaking into computers and hasn't stopped since. He loves nothing more than discovering new vulnerabilities, exploits and defensive techniques, meeting other security enthusiasts and simulating the latest cyber threats.

Pete

WEB APPLICATION HACKER

Pete pushes the boundaries of his skills at every given opportunity and has done for years. As an expert developer-come-hacker, he is a fount of knowledge when it comes to web-based technologies and happily shares it with everyone who will listen. Pete is so dedicated to the cause that if you were to ask him to defy the laws of physics, he would try everything in his power. Which means he regularly surprises his customers and fellow hackers with custom-made tools and impressive results.

Charles

INFRASTRUCTURE HACKER

Charles has been a Penetration Tester for years. He can't get enough of the adrenalin buzz when you defeat the defensive capabilities of a system and gain access to the objective. His career has taken him to a variety of organisations of varying types including high-profile companies. This experience gives him the capability to assess technical vulnerabilities and establish the risk this poses in the context of the customer's environment. Charles does a great job of expanding his knowledge and researching new problems and capabilities. He has achieved many different security certificates that he proudly has on his downstairs loo wall.

HOW WE ARE 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 YGHT, 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 YGHT, 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 YGHT, 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.

What is cyber threat simulation and penetration testing?

Penetration testing is the **art and science of hacking into an organisation's IT systems for its benefit**. Over time the term penetration testing has meant many different things to many different people. In general, they all mean some form of exploitation of cybersecurity vulnerabilities. The purpose of such activities is to make sure the owners of the IT system know what vulnerabilities are present. They can then understand the level of risk and then choose whether to take corrective action.

Penetration testing can feel arbitrary and contrived, which is understandable: real threat actors can take months to discover flaws and execute attacks. Penetration testing is done in as condensed a fashion as possible and can feel detached from any context. Threat simulation, on the other hand, takes the primary concepts of penetration testing and then applies them to a context set by the customer. The context determines how we perform our attacks and what the results mean. Sometimes we are given the luxury of taking longer to quietly complete the attacks, which helps the customer determine what was noticed by the defensive team. While on other engagements, we simulate only the most basic of attackers, in line with the organisation's needs. In all cases, the consultant ties the results to what they mean, not just an arbitrary score.

Who needs cyber threat simulation, penetration testing and other YGHT services?

Every person, computer, digital service and organisation from every country on this planet (and in orbit) are targets for the bad guys. All of those people, computers and services need protecting.

Any organisation that creates, provides or uses technology probably should use penetration testing services. Some organisations perform penetration testing because they are obliged by law, by standards compliance requirements, or mandated by client contract. Others do it just because they know it is the right thing to do for everyone!

What types of cyber threat simulation and penetration testing do YGHT offer?

We offer many different services here at YGHT, including penetration testing of infrastructure; web and mobile apps; and Internet of Things (IoT). Additionally, we perform a range of social engineering tests and other advanced security testing.

We also have technology called the Smuggle Box that allows us to remotely perform many different services that would traditionally be done while on site.

We can tailor our services to your exact requirements, so if you don't see what you're looking for, please ask us!

01 CYBER HEALTH CHECK

Members of management need to know that they are doing the right thing for their organisation's cybersecurity.

A Cyber Health Check is where YGHT's highly experienced experts discuss the current state of your organisations IT infrastructure and its cybersecurity with your technical staff. The experts will then perform an optional external vulnerability scan and create and deliver a report aimed at non-technical decision-makers. The report summarises the organisation's cybersecurity capabilities alongside suggested routes for improvement.

WHO?
Where management feel uneasy about their cyber security

WHAT?
A Cyber Health Check and vulnerability scan

WHY?
To get a weather-vane assessment of where you are now

HOW?
Video calls and presentations

02 WEB APPLICATION PENETRATION TEST

A Web Application Penetration Test is where YGHT attempts to break into a specific web application.

Web application tests are often an exercise in their own right. This is because the web site or application can be orders of magnitude more complex that the infrastructure that runs it. Splitting the two tasks allows the organisation to correct the problems identified, take a sigh of relief, regroup and move onto the next.

Web application testing is a different set of actions than infrastructure testing. The core concepts are similar, but the tools, techniques and procedures are very different. The simulated threat actors also differ. Infrastructure penetration tests assess the security of the organisation. While web application penetration tests also determine how vulnerable the users of the web application are.

WHO?
Any organisation that runs a web application

WHAT?
A web application test of the application and its supporting infrastructure

WHY?
To understand what a malicious user of the web application can achieve

HOW?
Remote consultants working over the Internet against your web application

“The guys at YGHT did a thorough job and made it possible for our development team to not only correct the problems identified, but also to improve their engineering skills to prevent similar vulnerabilities from occuring in the future. Very professional, would recommend!”

- Margaret @ Client A

CASE STUDY A

This client is a small organisation that develops and operates a web application that provides services online to companies throughout the UK. Their industry’s governing body requires them to perform annual web application penetration testing.

Each year the application is tested throughout with a particular focus on new functionality and vulnerabilities that have emerged since last year. The web application uses an older software framework. It has such a broad array of functionality that a replacement build would be challenging to achieve. Despite the restrictions of operating older software, the organisation continually strives to ensure they do not allow weaknesses and vulnerabilities to develop on their platform. Following each penetration test, the web application undergoes any corrective action needed. A month later a retest is completed to show that any identified vulnerabilities have been sufficiently corrected. When the system meets the governing body’s compliance requirements, a formal note is included in the report enabling the organisation’s continued compliance certification.

The skilled staff at YGHT made it possible for this organisation to understand their level of cybersecurity and achieve their compliance requirements. Now the customer has shown that YGHT’s guidance has enabled them to begin a successful continual improvement programme.

At YGHT, we take our client’s privacy very seriously. All projects are assigned code names, and we never reveal our clients’ identities to anyone else. Unfortunately, this means that we don’t have any case-studies that have our client’s business names in either. This is an anonymised case-study.

03 MOBILE APP PENETRATION TEST

Mobile application penetration tests analyse the security of a mobile app, focussing on ensuring client safety and network security.

During a Mobile App test, YGHT will examine Application Programming Interfaces (known as APIs): this is the technology that allows the App to talk to the cloud. These APIs are sensitive and present a substantial amount of the organisational risk. On more extensive Mobile App tests, it would also be appropriate to assess the code that makes up the App itself. Analysing the code allows a better understanding of the risk to users as well as the organisation.

WHO?
Any organisation that runs a mobile app

WHAT?
A mobile app test of the app and its supporting infrastructure

WHY?
To understand what unwanted impact a malicious user of the app can have

HOW?
Remote consultants working over the Internet against your app API and app code

04 INTERNET OF THINGS (IOT) OR DEVICE PENETRATION TEST

There's an ever-growing number of devices connected to networks or the Internet, and each of these devices is essentially a mini-computer. These mini-computers share many qualities with the rest of technology, including their susceptibility to a cyber attack. Unlike other IT systems, there are additional risks for consideration when consumers can physically interact with devices that don't occur with other systems.

Device penetration testing exercises can assess the technology's resilience to a variety of attackers and techniques. The service comes in a variety of forms which can be selected depending on the context of the device. The approach suitable for a connected Insulin Pump may not be appropriate for a Smart Fridge. For this reason, all aspects of a Device Penetration Test is made-to-measure.

WHO?
Any company that uses, develops, owns, or operates IoT or other connected devices

WHAT?
A Device Penetration Test against the device, firmware and supporting public infrastructure

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

HOW?
Remote consultants using destructive and non-destructive testing techniques against the end-device as well as performing simulated attacks against the Internet-facing support infrastructure

“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

This client develops and manufacturers high-end Internet-of-Things electronic devices for use at home. Their internal technology team is relatively small and does everything from software engineering to PCB design in-house, but does not do cybersecurity.

A cybersecurity researcher approached this client after identifying several severe flaws in the client’s systems. The researcher asked them to make corrections within 90 days before they intended to publish the results. Having no experience in cybersecurity, they did not know what to do. Nearly halfway through the disclosure period, they asked YGHT for help with several things.

The services the client needed ranged in technical depth. At the business end, they needed help gaining an understanding regarding what Responsible Disclosure means and how they should respond. While at the technical end, the client asked for a full assessment of their product and assistance validating their corrective actions based on the assessment findings.

In partnership with YGHT, the client managed to publish major fixes to their services and all their deployed devices before the 90 days Responsible Disclosure period was over. These fixes included completely re-writing the cryptography routines as well as changing the way that the system created and handled credentials.

At YGHT, we take our client’s privacy very seriously. All projects are assigned code names, and we never reveal our clients’ identities to anyone else. Unfortunately, this means that we don’t have any case-studies that have our client’s business names in either. This is an anonymised case-study.

05 INTERNAL PENETRATION TEST

Internal penetration tests assess what happens when an attacker has access to your internal network. Cybersecurity experts consider such an attack to be a matter of time before an attacker gains access, whether that be an unknown external attacker or a rogue employee. It involves probing part or all, of the systems that live inside the organisation's network perimeter. Often companies have done some work to protect themselves from attack over the Internet, but internally, is typically a completely different story.

Internal penetration tests are reasonably unconstrained, in terms of targeting, and the technical objectives. It is up to YGHT to work out what asset is the most sensitive and essential to the organisation. Don't worry; we always treat the information we find with due respect. For example, we only take the minimum amount of agreed data to be able to show the outcomes in our reports. If we put this data into our report, the data is always anonymised.

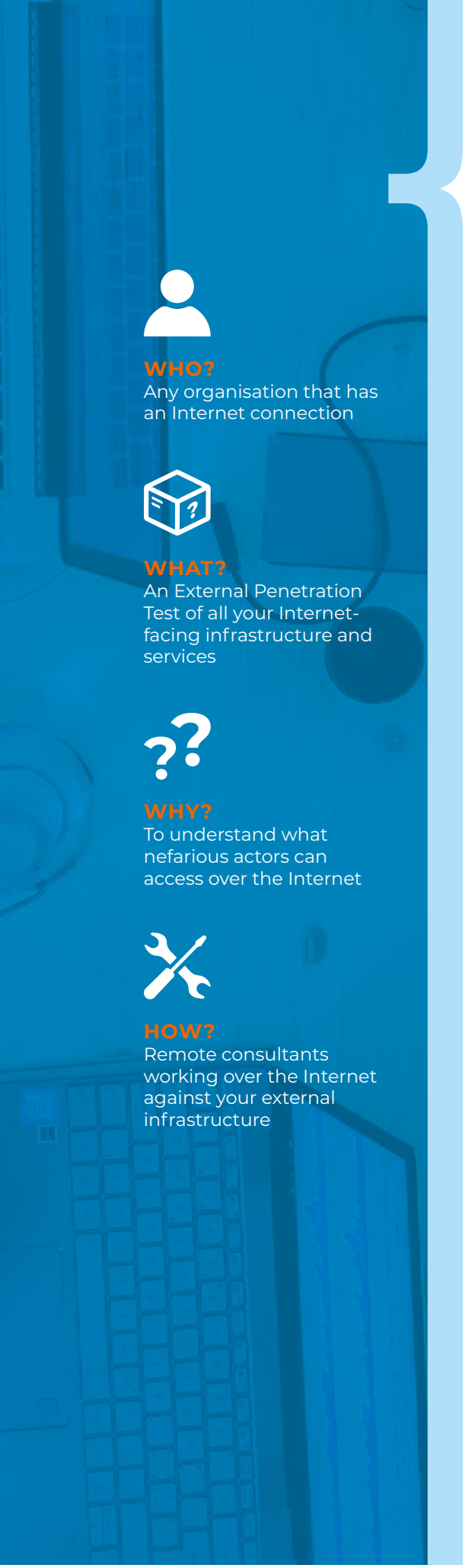
Significant cybersecurity concerns can be found in what appears at first to be unlikely places. Internal penetration tests are the most likely place to discover "chained" vulnerabilities. A chained vulnerability is where one minor vulnerability, leads to another, which might lead to yet another vulnerability, in total, the minor vulnerabilities result in a significant impact.

WHO?
Any organisation with an IT network

WHAT?
An internal penetration test of some or all of your IT networks

WHY?
To assess what damage an attacker can achieve when they breach the perimeter

HOW?
Remote consultants using a SmuggleBox as their foothold in your network



06 EXTERNAL PENETRATION TEST

Most organisations carry a large proportion of their cyber risk at their perimeter to the Internet. This risk is owing to the sheer quantity of potential attackers to which Internet-facing systems are exposed. External-only penetration tests can be used to start a cybersecurity programme because it assesses the attack surface that can be affected by the most prolific threat. If an organisation hasn't done much testing before, this is a perfect place to start. In most cases, it is a bite-sized chunk that can help establish what is needed for a successful penetration testing programme to be completed.

Any penetration test is an activity that attempts to break into a given set of systems. An external penetration test specifies that the systems in-scope for testing are only those that are Internet-exposed. Typically this activity relates to the infrastructure in place to run systems such as email services, VPNs and remote access facilities as well as the servers that run web sites.

WHO?
Any organisation that has an Internet connection

WHAT?
An External Penetration Test of all your Internet-facing infrastructure and services

WHY?
To understand what nefarious actors can access over the Internet

HOW?
Remote consultants working over the Internet against your external infrastructure

07 WIRELESS NETWORKS AND NETWORK SEGREGATION TESTING

One crucial element of cybersecurity is configuring network segregation and segmentation correctly.

Network segregation is a desirable quality as it helps stop a successful attacker from being able to spread around the inside of your network. Separating the network such that there only controlled communication between areas is permitted is the most effective way of segregating networks. Wireless network assessments typically include segregation testing as guest wireless networks often should not be allowed access the internal network.

Wireless network penetration tests also assess the access control mechanisms and cryptography in use. As wireless networks get used very differently, the context of the network directly influences the types of cybersecurity tests performed.

WHO?
Any organisation that users WiFi networks

WHAT?
A wireless segregation and access control test against chosen physical locations

WHY?
To examine how attackers could use WiFi to gain access to company services

HOW?
An onsite consultant using specialist equipment to attack WiFi networks

08 BUILD STANDARD ASSESSMENT

Build-standard assessments require that the YGHT assessor has a copy of the target device to look at the configuration. With this information, they can work out if it is weak to any known problems.

The assessor can then go further, looking at ways of hardening the build, so that unknown, or future vulnerabilities are less effective. Many different attacking perspectives are used in a build-standard assessment. Examples include simple attacks such as theft of the device, all the way to how easy it would be for nation-states to spy on network communications.

WHO?
Organisations that frequently deploy equipment in a variety of settings

WHAT?
A build standard assessment of a laptop, server, or firmware image

WHY?
To determine the level of security present on any standardised device

HOW?
Remote consultant, working against a virtual machine, laptop, or other device

“We thought we were pretty safe. We had been getting a penetration test fairly regularly for several years. YGHT really did Hack That and showed us that we were resting on our laurels. Thank you for giving us the motivation to do better.”

- Grace @ Client C

CASE STUDY C

This client owns a global network of connected devices that provide security services to tens of thousands of buildings. Each device is standard hardware and firmware that has been altered to suit the specific needs of their network.

The device was initially only subjected to network and configuration testing to see what services were exposed and what vulnerabilities were immediately evident. As there were some initially worrying results, the client increased the scope of the work to include initial firmware extraction and analysis at which point several serious problems were confirmed.

YGHT worked with the client not only to identify the vulnerabilities in the first place but then to help the management understand the implications of these vulnerabilities. Following this, the client was able to prioritise corrective actions and put other protective measures in place where no corrective actions were possible.

At YGHT, we take our client’s privacy very seriously. All projects are assigned code names, and we never reveal our clients’ identities to anyone else. Unfortunately, this means that we don’t have any case-studies that have our client’s business names in either. This is an anonymised case-study.

09 VULNERABILITY ASSESSMENTS

Vulnerability assessments are useful in three circumstances: where budget constraints don't allow for penetration testing at all; to periodically check the vulnerability level of computer systems to make sure things haven't developed obvious holes; and where comprehensive penetration testing would be prohibitively expensive owing to the sheer scale of the network.

Performing a vulnerability scan is where YGHT launches specific tools against a set of targets in one of two ways: authenticated or unauthenticated. Authenticated scanning is where the vulnerability scanning software logs into the system and performs an in-depth search for potential issues. In contrast, unauthenticated scanning just observes the problems exposed to the network. Typically, internal vulnerability scans are authenticated, and external vulnerability scans are unauthenticated.

WHO?
Any organisation that either has a limited budget or needs a regular review

WHAT?
Internal and external vulnerability scans against relevant infrastructure

WHY?
To get a high-level technical assessment of the vulnerabilities present

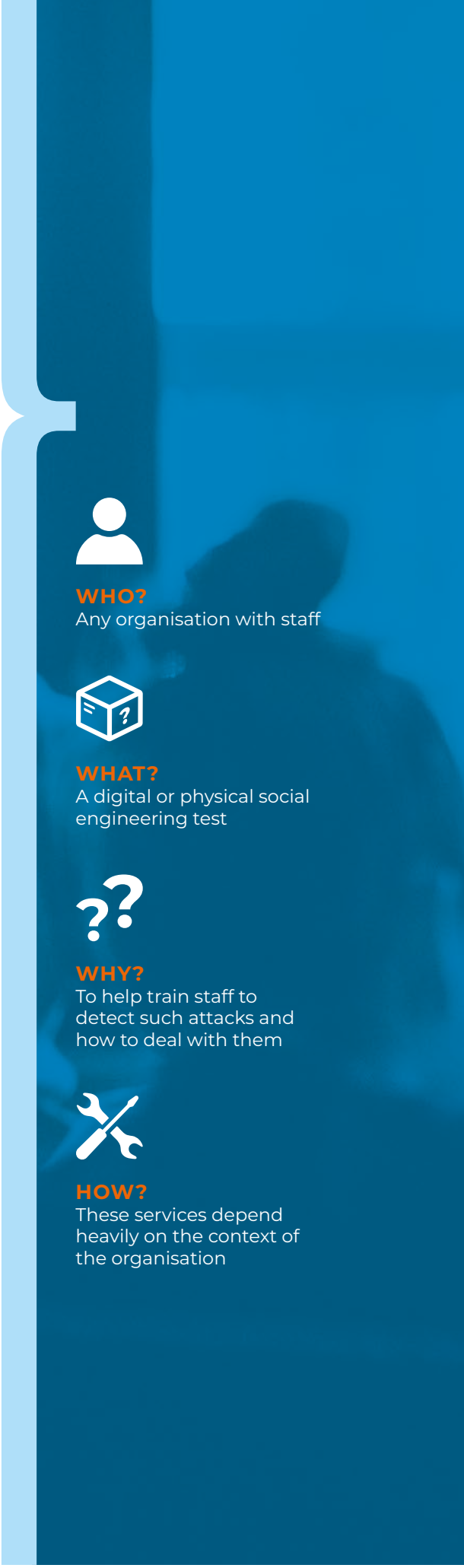
HOW?
Remote consultants working over the Internet against the infrastructure or with a SmuggleBox on the internal infrastructure

10 DIGITAL AND PHYSICAL SOCIAL ENGINEERING TESTS

These two types of work are where the people at the organisation are the focus of the test.

We look at how well members of staff can cope with people trying to get them to do things that they usually wouldn't. Physical Social engineering exercises range but often involve finding your way to an area of the organisation. For example: being let through reception without being greeted by a member of staff; or having someone hold open the back door for you as they go out to smoke.

Digital social engineering tests have a few forms. One type of test is where the attacker sends semi-targeted phishing emails to all members of staff. In contrast, targeted spear-phishing campaigns are where the attacker builds up a rapport with individuals first before getting them to perform a risky action. The threats simulated by these exercises are typically performed by real attackers very early in a breach. This realism particularly applies to email-based attacks, which makes them useful risks to understand.



WHO?
Any organisation with staff

WHAT?
A digital or physical social engineering test

WHY?
To help train staff to detect such attacks and how to deal with them

HOW?
These services depend heavily on the context of the organisation

11 ADVERSARIAL INCIDENT TESTING

Generally speaking, cybersecurity specialists don't talk about "if" an attack takes place, but "when". With this mindset, it is essential to know how well technical staff perform in an incident.

Adversarial incident testing focuses on whether the IT team detected an attack, how they respond to it, and what technical failures there were in terms of forensic capabilities.

Organisations that are higher on the cybersecurity maturity model should actively seek to validate their detection and response capabilities. Adversarial incident testing artificially creates a security event. The defensive team should detect the event which then allows them to safely test their tactics, techniques and procedures when such an incident occurs.

WHO?
Organisations that have a mature security stance

WHAT?
Adversarial incident testing

WHY?
To exercise the capabilities of the Incident Response team in a controlled fashion

HOW?
The methods used will be dependent on the context of the organisation and will be agreed with the customer

12 RED TEAMING EXERCISES

Red Teaming exercises are designed to establish the security of the organisation on several different levels and angles. This type of testing is the gloves-off, no-holes-barred security assessment, where the only thing that isn't permitted is Denial-of-Service (DoS) attacks. A Red Team exercise with YGHT will inevitably test your people, your software, and your networks.

Red team exercises aim to gain access to crucial organisation assets without being detected. This type of security assessment simulates a real attacker as closely as possible to push the organisation's defensive capabilities. The information generated by these exercises shows what activity was detected, how it was caught and crucially the actions that were not seen - all focusing on the defence of those crown jewels.

Red Teaming exercises tend to be a more extensive scale, with slow laser-focused actions and can span weeks or months. This sort of work is not for the faint-hearted, but, it is the Gold Standard for understanding how well protected the organisation is from an aggressive and highly targeted cyber attack.

WHO?
Organisations that have a mature security stance

WHAT?
A Red Team exercise

WHY?
Because real determined attackers aren't constrained like penetration tests

HOW?
The methods used will be dependent on the context of the organisation and will be agreed with the customer

“Before using YGHT, we always worried that our penetration testing provider couldn’t keep up with our frequent requirements and varied demands. Now we use the team at YGHT, those worries are gone. We can’t thank them enough for being a pleasure to work with as well as being highly effective and educational.”

- Adiel @ Client D

CASE STUDY D

Client D operates a large IT estate. Including general head office equipment, a small data centre, hundreds of public-facing premises throughout the UK, and several large-scale web applications which integrate with numerous partner platforms.

This client undertakes a variety of penetration tests each year, focusing on different areas of the business. The internal security team has a strong defensive capability but understands that their skill set does not include threat simulation and offensive actions.

Each web application test is complex. The boundaries of the test have to be established, which requires technical discussions with third parties and agreements to be drawn up. The technologies used varies between systems; some heavily use client-side script languages and web sockets. In contrast, others are more traditional RESTful applications.

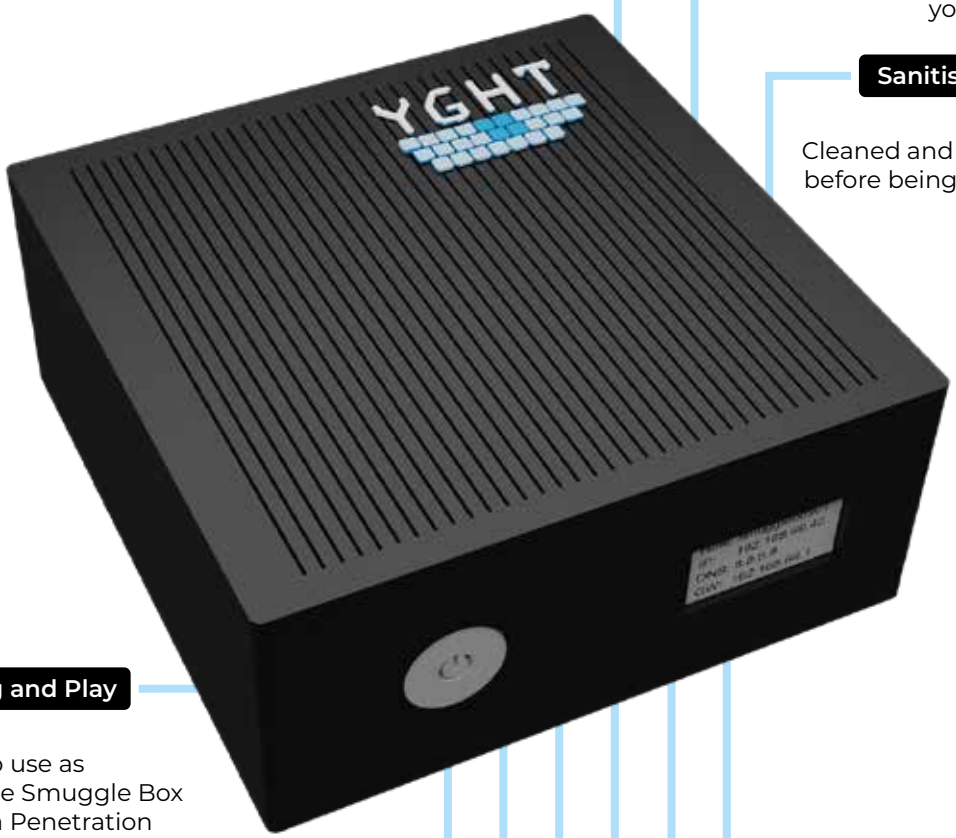
Each year a sample of the premises are subjected to a Physical Social Engineering test where the objective is to drop a device onto the companies network. The network is subjected to a technical assessment once the consultant’s device is in place. The exercise establishes the attacker’s level of access to the target’s network, and what impact a successful attacker would have.

Penetration testing is performed against the IT at the head office and the data centre after the completion of each of the IT department’s development milestones. The purpose of each test is to measure the organisation’s progress towards its security goals. They operate a sizeable technical estate and recognise that their level of security maturity is not as high as they would like. With the specialist insight that YGHT provided, the organisation was able to determine which path they needed to take and has made substantial improvements.

At YGHT, we take our client’s privacy very seriously. All projects are assigned code names, and we never reveal our clients’ identities to anyone else. Unfortunately, this means that we don’t have any case-studies that have our client’s business names in either. This is an anonymised case-study.

SMUGGLE BOX

The **Smuggle Box** is a device that allows your expert penetration tester to remotely perform their duties against the inside of your network. Internal penetration testing allows you to understand what impact an attacker could have after they complete the initial cyber security breach.



Built For You

Each Smuggle Box is new for you and only you, no digital components are reused.

More Flexibility

The technical and operating flexibility allows for services to be completed that fit your needs.

Sanitised

Cleaned and sanitised before being shipped.

Plug and Play

As simple to use as plugging the Smuggle Box in, just like a Penetration Tester would with their laptop on site.

Data Sovereignty

Data is stored internally and your trusted consultant adheres to high Data Sovereignty values and ethics.

Full Disk Encryption

No third party can tamper with the device in the event of theft or loss.

Heavily Encrypted Connection

High strength communication encryption (TLS) to ensure no eavesdroppers can steal data.

Lower Cost

No consultant on site? No expenses to pay!

Secure

Built to internationally recognised security standards to ensure a very high security device.

Stay In Control

Option to purchase storage components for your own data destruction routines once services are complete.

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.

SERVICES WE DON'T OFFER

Here at YGHT, we know our strengths. Those strengths exist because we continually hone and develop them. What this means is that there are some things we don't do which you should know about:

Standards Compliance Work

We don't do standards compliance such as ISO 27001 auditing or PCI-DSS implementation because, frankly, it isn't as much fun as hacking into things. Keeping hacking skills sharp means there is no time to study much else. But don't worry, all our penetration tests can support a standards compliance programme. If you need standards compliance work, still get in touch: we have trusted partner companies that we can put you in contact with.

Remediation or corrective-action work

Our skill set is best suited to offensive, rather than defensive cybersecurity. While we can make systems more secure, there may be more inspired ways to do it. On top of that, there is a fine line to tread to help you as best we can without getting into any situation where we are testing the security we put in place.

Incident Response

We often can't get involved in Incident Responses because of timing, though we would love to help if we could. Inevitably when we get asked to help with Incident Response, we have 6 weeks of client work lined up, which makes it very difficult for us to be of any real use. Please do ask, as if nothing else, we will point you in the right direction

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 us: helpme@yg.ht **Call us: +44 161 818 9448**

FAQS

Will you break our system?
It is impossible to say that penetration testing won't break your system; however, it is unusual. Anything intrusive will test the limits of any system. We don't perform load testing or Denial of Service (DoS) testing unless requested. When we prepare the scope of the penetration test with you, please tell us if you have particular concerns about a system breaking. We can usually adjust our plans to suit or advise you accordingly.

We don't have much of a budget, can you still help?
Any penetration test is better than no penetration test, so "Yes!" - get in touch. We might suggest that the best course of action is to do a sampled penetration test rather than an exhaustive one. Alternatively, we will help you scope the most critical assets for prioritised testing.

We need quite a lot of work doing, can you deliver it?
Probably, but this depends on many factors. For example: when you need the work completed; what sort of work it is; and our current workload. Get in touch with us as early in your project as you can so that we have a better chance of arranging what you need.

How long does a penetration test take?
We do know that it is unusual for a single penetration test to be less than three days or more than 20 days. Most fall somewhere in between. The length of a penetration test entirely depends on the type of target and how complex it is.

What happens if you find something serious?
We get in touch as soon as we understand what we have found. Being prompt is essential for two main reasons. Firstly, the vulnerability affects your systems, it is your choice how to proceed with the exercise, and we will present your options to you. Secondly, we don't want to take the risk that the vulnerability gets taken advantage of before you are aware.

What happens if you find evidence that someone else has already breached our system?
Thankfully this doesn't happen very often; however, it can and has happened. Should this happen on your test we will stop the test and immediately get in touch with you. Breaches have less of an impact if quickly contained so we will work through your options with you and support you as best as we can.

Do I legally have to own the systems that we want you to test?
It is easier if you do. When testing third-party systems, the third party has to agree beforehand. In these circumstances, we will have discussions between all parties. We will make sure we all agree on several key factors. These include the test boundaries, ensure everyone understands the type of work, who gets the results, and so on.

Can you work in the evenings or at weekends?
It is possible, at an additional cost, but only when unavoidable. If you need us to work out of standard hours, we will need a technical representative of your own to match those hours.

What are the main stages in having a cyber security test?
1. Scoping
2. Start brief
3. Execution
4. Reporting
5. Debrief

How secure are you, and what is your data retention period for our data?
We take security very seriously and practice what we preach at every opportunity. Don't be surprised to find that we do things differently, we are continually looking for ways of pushing the boundaries of cyber defence and regularly implement new capabilities. We are certified to the UK government's Cyber Essentials Plus standard. However, this must is considered a bare minimum standard that we surpass by a long way. We destroy all raw data after a maximum of 3 months and only retain the minimum amount of anonymised data after this point.

How often should we have a penetration test completed?
You might find that you have a contractual, legal, regulatory, or standards compliance requirement that determines when and how frequently you should have a penetration test. Often this is once per year per scope or after any significant change. We find that most organisations use this strategy even if it isn't an external requirement. That doesn't mean you can't have more frequent tests though."

Who is the best person in our organisation to help you make the penetration test go smoothly?
As all organisations are different, there is no hard and fast rule about who should coordinate a penetration test. We find that a technical audience is usually the best to help with the details of the systems, and the IT or security manager is best for the strategic elements of a penetration test.

We've heard about "commodity penetration testing", is this good enough?
Maybe, but this depends on your requirements. Commodity penetration testing is reasonably standardised, it can be very checkbox oriented and you may find that you are left wanting more. At YGHT, we only offer consultant-led penetration testing, which means you always get an expert's opinion and guidance on what courses of action you can take. Being consultant-led also ensures that we can adapt and compensate should anything unusual happen in your test. We strive to always deliver what is best for you and your systems.

We do Vulnerability Scanning; do we need a penetration test as well?
Probably. Vulnerability Scanning is a tool to automate the process of identifying software that is affected by known vulnerabilities and is most useful when performed often. However, it is no substitution for the human intellect. Security isn't just about making sure all your software patches are up to date but don't get us wrong, this is very important.

We know we need cybersecurity, but we don't know what, can you help?
Almost certainly, don't worry about not knowing what to do next - cybersecurity is a vast subject!

Can you customise the work and the report for us?
Absolutely. We have a way of approaching things that usually hits the spot, but, we are consultant-led, so anything is possible. We remain flexible and agile to give you what you need.

How do we securely transfer information between us?
We have several options. You can choose from a range including emailed encrypted ZIP files with a passphrase sent via text or another method; GPG encrypted emails; or cloud services such as O365. Let us know what you need.

How do you take payment?
Bank transfer is our preferred method, though if this is not suitable let us know, and we can discuss alternatives.

Can we tell anyone you did our penetration test?
We would love you to! Some organisations don't want to be associated with cybersecurity services, but we think this may harm your reputation. You should tell people you have penetration tests completed because there is increasing public demand for better care of data.

The estimated cost you have given us is significantly different from another quote; why might that be?
Good question! There could be many reasons so to find out for sure get in touch with us. Some examples include:

- the quote is for a different scope
- we may have realised that an element of the exercise is going to be challenging or more straightforward than it first appears
- or one quote is for the test to be a representative sample of your system rather than the whole thing.

In any case, get in touch, and we will work it out.

What is the difference between Black Box, Grey Box, and White Box tests?
These are three overall ways to approach a penetration test. White Box tests are where all information, including items such as code and network diagrams, are shared with the consultant before the test. Black Box testing is where the minimum legal information is shared with the consultant before the test. Grey Box testing is somewhere in the middle. The reason these approaches exist is because each has its positive and negative points. White Box testing can dampen the creativity of the consultant, so fewer vulnerabilities may be found but does allow complex systems to be understood quickly. In contrast, Black Box testing enables the consultant to mirror the behaviour of a real attacker much closer and so can lead to interesting and useful results.

What additional costs should we expect?
There aren't usually many additional costs, but it depends on many factors. If you need us to be on-site, there will be travel and subsistence expenses. If your test requires us to create infrastructure on the Internet, purchase domain names and so on, these costs are not usually high and will be chargeable.

Should Intrusion Prevention Systems (IPS) be enabled for a penetration test?
Not usually. During a penetration test, IPS systems mask the true defensive capabilities of the system. Having a true-to-life assessment might be what you are looking for, but most of the time, this isn't a desirable bias. It may not be possible to disable an IPS if you are reliant on an IPS because of known vulnerabilities. If this is the case, let us know, and we will work through the options you have.

Do you perform load testing or Denial of Service (DoS) testing?
Not usually, but if we spot something that might indicate issues, we will let you know. System load is a complex subject and should be considered a test of its own. A range of factors creates this complexity, so any meaningful test needs to be well thought through to get useful results. DoS attacks are well known to be possible with utterly vast amounts of resources. You should assume that if an attacker wants to Deny your Service, they probably can.

Printed on 100% recycled paper.

Cyber security confidence starts here.

Contact You Gotta Hack That today to discuss your cyber threat simulation and penetration testing needs.

Visit
yougottahackthat.com

Call
+44 161 818 9448

Email
helpme@yg.ht

You Gotta Hack That

Registered address: 112 - 114 Witton Street, Northwich, Cheshire, CW9 5NW • Company number: 10722704 • VAT number: GB 280 3908 00