chess® Helps You

Work From Anywhere

Secure Your Homeworkers

with Remote Access Penetration Tests

What is a Remote Access Penetration Test?

A remote access penetration test is a type of external penetration test, which searches for vulnerabilities that can be exploited by a hacker and replicates a real-life attack.

This type of analysis aims to target everything Internet-facing. The typical objective is to gain internal access to the network.

Attackers will:

1. Target exposed services on public IPs
2. Try to gain access to Office365
3. Use phishing/vishing
4. Exploit vulnerabilities in home networks

Did You Know?

> Chess is certified by The Council for Registered Ethical Security Testers (CREST), a non-profit organisation which aims to bring high quality and constancy to the global technical cyber security sector.

What Are Your Options?

This penetration test service has four tiers and you can choose which option suits your your organisation best:

Remote Access Break-In Penetration Test

The main objective of this type of penetration test is to obtain internal access to an organisation's network.

It will test the outer layers of defences your company has put in place to protect remote working such as your remote access system, Citrix, Office 365, etc.

Compromised Homeworker Penetration Test

The main objective of this type of penetration test is to assess what a hacker can achieve if they bypass the remote access systems security controls and successfully gain internal access to your organisation's network.

It exploits the possible misconfigurations of a rushed remote working roll out and checks what the VPN connection could be a path to.

External Vulnerability Assessment

The objective of this scan is to asses and highlight vulnerabilities in your public facing infrastructure which may provide a route into your network.

Vulnerabilities are scored by priority and remediation advice is provided.

+ +

Remote Access Penetration Test Bundle

This is the most advanced option which combines all three approaches and tests your system for various vulnerabilities that may have opened when you've rolled out remote working.

Why Do You Need It?

In light of the recent COVID-19 pandemic, companies are enabling remote working at larger scales. For businesses to continue to operate, speed is vital in the current situation, and IT are faced with resource challenges to mass roll out remote access.

Often security is left as an afterthought and attackers take advantage of the newly created vulnerabilities in the system and the social panic.

Through a Remote Access Penetration Test, you will:

- **Identify vulnerabilities** that can be exploited by malicious actors
- **Improve your business security** stance and reduce the risk of attack and data loss
- **Provide reassurance that your staff** are working to best practices even when working from home
- Help to **highlight areas that can be improved** using your existing security product licences and technology to achieve a return on investment
- Help to **preserve your brand** and reputation.

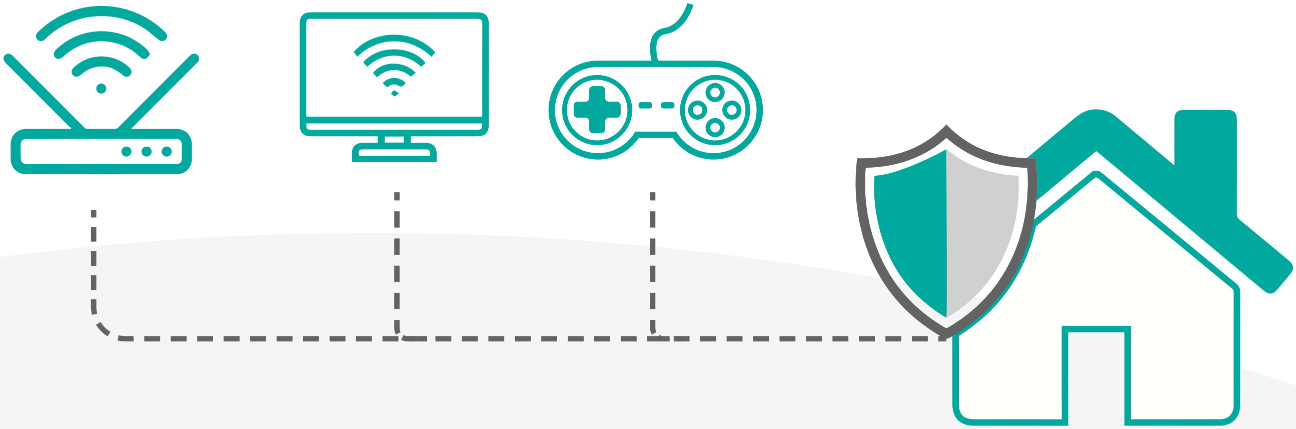
Security Vulnerabilities in Home Networks

Employees working from home can expose your network to a wider set of threats.

Home networks are predominantly insecure:

- People tend to use the default settings on their router which do not provide the highest level of protection
- With the increase of smart home appliances, the home attack surface is increased, and hackers can use your smart TV to gain access to your home network
- Children nowadays are often technically versed and can adjust settings to optimise their gaming experience but open the home network to attacks.

To protect your business system even if the home network is compromised, as an organisation, you need to ensure you have a secure baseline configuration for home use devices, advanced endpoint protection and multi-factor authentication in place to reduce the risk of an attacker gainining access to that system and into the office network.



What is the process?

Chess Remote Access Penetration Testing Methodology

1. Scoping

Chess will schedule an online call and work with your organisation to define the scope of the engagement.

2. Test Plan

The assigned Chess engineer will create a detailed plan explaining how the penetration test will be executed and what exactly is going to be targeted in your organisation.

3. Penetration Test Execution

No internal or physical access is required. The penetration tester will test your system from a remote location.

The objective of the penetration test will depend on the option you choose. At this stage the engineer with use automated tools, manual testing techniques or a combination of both.

The objective would be to identify a range of potential vulnerabilities in an organisation's target systems, which will typically involve the Chess engineer examining:

- Attack opportunities and routes, plus threat agents (e.g. new home workers who don't have the habit of following basic cyber hygiene outside the office)

- Technical system/network/application vulnerabilities (e.g. vulnerabilities in your endpoint or firewall protection and lack of multi-factor authentication).

Once vulnerabilities have been identified, the Chess engineer will attempt to exploit them to either gain internal access to your system or explore what damage an attacker who's already gained access can do.

4. Reporting

Chess will provide a detailed penetration test report, detailing any threats or vulnerabilities found and the recommended remedial actions. Threats and vulnerabilities will be ranked in order of criticality. The report will also contain an executive summary and attack narrative, which will explain the risks in business terms.

5. Follow-Up Call

The Chess engineer will present the report to the key stakeholders within the organisation on a conference call and explain in business terms what the actions are required to protect your system from outsider threats.

Chess can provide additional consultancy, products and services which can further improve your organisation's overall security stance.

Did You Know?

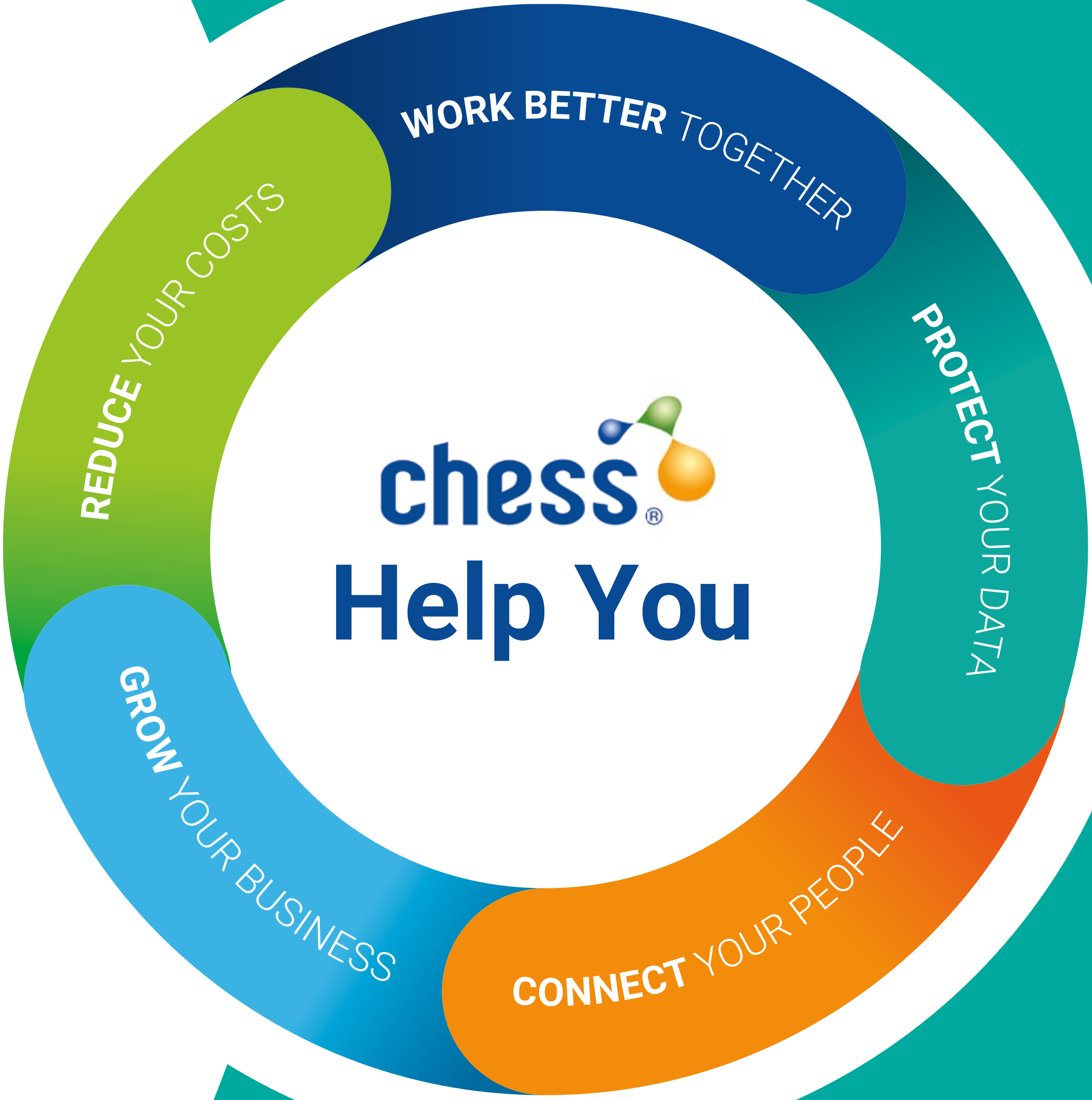
> A remote access penetration test does not require any internal or physical access. The penetration tester will test your system from a remote location and try to gain internal access to your network.

About chess®

Chess is one of the UK's leading independent and trusted technology service providers, employing 480 skilled people across 6 UK sites, supporting a wide range of organisations.

By leveraging world-class technology, Chess helps you to connect your people, protect your data, grow your business, reduce your costs and work better together, which means your business, your people and your customers can thrive.

At Chess, we're passionate about our unique culture and our continuous investment in our people to be industry experts. We're extremely proud that our people voted us No.1 in 'The Sunday Times 100 Best Companies to Work for' list 2018, and we continue to celebrate more than ten years in the top 100.



chess Help You

WORK BETTER TOGETHER

PROTECT YOUR DATA

CONNECT YOUR PEOPLE

GROW YOUR BUSINESS

REDUCE YOUR COSTS

chess® Helps You Work From Anywhere

Contact Our Team Today

✉ WorkFromAnywhere@ChessICT.co.uk

☎ 0808 252 0755

➚ ChessICT.co.uk/

chess®