SECURITY TESTING

WE FIND YOUR WEAKNESSES BEFORE THE CRIMINALS DO.

Penetration Testing is consistently proven to be the most effective way of identifying vulnerabilities and risk to your cyber security. Certified experts will perform controlled, simulated attacks against your company using real world hacking techniques to discover weaknesses in your systems.

"In 2021 80% of breaches were conducted by Organised Crime Groups (OCG's). It is documented that 29% of companies impacted by ransomware attacks were forced to make large scale redundancies."

Every weakness found in your systems is meticulously documented and quickly relayed to your team. Technical remediation advice and reproduction steps allow you to rapidly and effectively reduce your risk.

The work doesn't end when the findings are delivered. Direct access to Westcom technical advice before, during and after each test is a core part of our service.

External Testing

WESTCOMNETWORKS

External security assessments focus on the security of your public facing and internet accessible systems and services. These systems present access points into your internal network. Ensuring their protection from the latest threats is critically important to overall organisational security.

"Initial Access Brokers (IAB) carry out mass internet based attacks so they can sell network access to ransomware gangs."

Using industry standards as the basis of our external infrastructure methodology, experienced ethical hackers will assess your infrastructure for hundreds of vulnerabilities including:

- **Missing software patches** that introduce security vulnerabilities
- **Weak passwords** will be identified on public facing services such as RDP or SSH
- **Insecure configuration** of exposed systems resulting in decreased security for both users and the organisation
- **Exposed services** that can leak data or provide unintended network or data access

Internal Testing

WESTCOMNETWORKS

Disgruntled employees, compromised email accounts, remote access solutions, Internet accessible vulnerabilities, phishing and many other attack vectors can result in an intrusion into your private corporate network.

"Cyber attacks against corporate networks have increased by 50%. There will be a ransomware attack every 11 seconds in 2022, showing a year-on-year increase of 62%."

Internal Network Security Assessments evaluate the security of your company's internal systems and the ease and likelihood of their compromise. The evaluation includes a review of your company's entire network and Active Directory, as weaknesses in computer platforms and other innocuous devices can lead to the compromise of your company's critical data.

Our internal network methodology is designed to identify hundreds of vulnerabilities including those that are regularly used by real-world attackers to compromise networks and data. We review every component of your network including:

WESTCOMNETWORKS

- **Missing software patches** from Microsoft and third party software providers
- **Active Directory** vulnerabilities in AD structure, GPOs and role provisions
- **Lack of access controls** that allow the compromise of critical data
- **Sensitive data storage** resulting in access to sensitive at-rest data
- **Weak passwords** will be identified on AD and local accounts
- **Insecure Configuration** of software such as Microsoft Office that can allow malware to take hold of systems

Phishing Simulations

WESTCOMNETWORKS

Phishing simulations help guard your business against one of the key entry points to your network for attackers – their email inbox.

"A 2021 report carried out by Cisco highlighted that at least one person clicked a link within a phishing email in around 86% of organisations."

Once inside an employees account, on average it takes 212 days for companies to discover the breach, during which time attackers may have had full access to sensitive data and the opportunity to move sideways within the organisation into other accounts and systems.

Running regular simulations helps train staff to recognise, avoid and report threats entering their email inboxes all in a safe environment.

Westcom can run phishing simulations on a one off or better still on a recurring basis to ensure that cyber attacks are always fresh in people minds.

PCI DSS Testing

WESTCOMNETWORKS

Payment card details are an extremely valuable commodity to modern hackers, who will sell on stolen details to the highest bidder. If your organisation is processing credit card details, you must safeguard this data with robust controls and processes.

"The amount of credit card data available on the dark web increases by 135% each year."

Payment card details are an extremely valuable commodity to modern hackers, who will sell on stolen details to the highest bidder. If your organisation is processing credit card details, you must safeguard this data with robust controls and processes.

A PCI DSS Penetration Test will rigorously test for any exploitable weaknesses in your card data security. Precursor use a mix of industry leading automated tools combined with manual testing.

Built on the PCI DSS Penetration Testing standard, our PCI DSS Methodology will review your card data environment across three distinct areas:

- **Application Layer** testing will review web applications and API's used to handle card data
- **Network Layer** testing will review the underlying infrastructure used within your card data environment for vulnerabilities
- **Segmentation testing** will ensure adequate technical controls are used to restrict access to your card data environment

CONTACT US FOR MORE INFORMATION

SALES@WESTCOMNETWORKS.CO.UK

03300 555 665