COGNISYS
Smarter Cyber Security

# Red Team Exercise

Test the true strength of your defences, technology, people and processes, by simulating the actions of a cyber attacker.

Penetration testing is a valuable part of your cyber security defences, however a Red Team Exercise goes a step further. Our exercises can test the full spectrum of organisation policies, processes, and technology defences.

Significantly more sophisticated than penetration testing, our cyber attack simulation accurately mimics advanced, covert, multi-phase attacks which occur in the real-world.

After agreeing specific targets, our ethical hacking team execute a program for achieving the compromise, which can include elements from a full scope of blended attacks, selected to give the best chance of a successful outcome.

Continued overleaf...

01422 416 000
sales@cognisys.co.uk
cognisys.co.uk

## Technical Elements

Once the targets and scope have been agreed, the service can include:

- Open Source Intelligence (OSINT) gathering.
- Building, organisation, network, physical controls and system reconnaissance.
- Manual testing using the tactics, techniques and processes of a malicious actor.
- Attempted physical breach of the organisation's premises.
- Human targeting through social engineering.
- Hardware vulnerability exploitation.
- Wi-Fi network intrusion.
- Signal vulnerability exploitation e.g. RFID door-pass cloning.
- Business application exploitation.
- Zero-Day hunting and exploit development.
- Pivoting using compromised hosts for lateral movement through the network.
- Data insertion and exfiltration.
- Establish post-exploitation persistence.

Typical outputs include: results of reconnaissance, attack vectors chosen, attack methods, attack payloads used, attack results, short and long term mitigations, plus remediation.

## Key Benefits

- Improve your security posture. Go beyond typical pen testing to gain a deeper understanding of your likely attack vectors.
- Verify your security controls. Tests are against technology and employees, revealing your ability to detect and respond to attacks.
- Prioritise your risks. Understanding the most critical security issues to prioritise your remediation efforts.
- Reduce your risk. Modelling our exercise on real hacker behaviours provides greater visibility into your organisation's weaknesses.
- Achieve greater defensive agility. Use the outcomes to reduce the probability of a successful attack.

We're proud of our Red Team, which is made up of some of the most qualified people in the industry.

Our technical ability combined with our deep understanding of the techniques used by cyber criminals allows us to deliver a valuable service to protect you and your organisation.

## Report

Cognisys presents its findings in a comprehensive yet simple report format.

This typically comprises: an executive summary, methodology, technical findings, and prioritised recommendations for remediation.

01422 416 000
sales@cognisys.co.uk
cognisys.co.uk

INTERNAL PENETRATION TESTING | EXTERNAL PENETRATION TESTING | WEB APPLICATION SECURITY TESTING | MOBILE APPLICATION SECURITY TESTING | CYBER SECURITY REVIEW | RED TEAM EXERCISE | PHISHING SIMULATION | DARK WEB MONITORING | LOST OR STOLEN DEVICE ASSESSMENT | WIRELESS SECURITY ASSESSMENT | CLOUD SECURITY ASSESSMENT | MICROSOFT 365 TENANT REVIEW | ATTACK PATH ANALYSIS | OSINT ANALYSIS | CYBER ESSENTIALS | GOVERNANCE & COMPLIANCE | VIRTUAL CISO | MANAGED SECURITY | SMARTSCAN | SMARTVIEW