RED PENETRATION

Contract security consultancy services offered:

We are happy to offer any of the following services on a remote basis, and other requirements can be discussed on request. Services can be delivered by our consultants alone or as a temporary member of a project team.

Working hours can be arranged to suit your requirements.

For further information, email hello@redpenetration.com or call +44 161 818 4575

Web application

- Simple and complex web application assessments on the majority of platforms.
- We have a consultant with OSWE if desired by clients.

Mobile

- Android / iOS / iPadOS apps.
- Have also tested Nokia / Windows phone / Windows Mobile / Windows CE / Blackberry.
- Have various stock / rooted / jailbroken devices in my drawer and can deliver mobile testing from them.

Network

- Internal and external network testing.
- Can perform testing remotely via a VM or physical device.

AppleTV / Samsung TV / Android TV

Thick client / compiled app / appliance / SaaS instance

- We have tested lots of Java / .Net / Native thick clients and other software in the past.
- We have bypassed licensing systems and retrieved crypto keys.
- We have tested Linux / Mac thick clients before too.

Hardware

Physical security devices

- RFID / NFC access control.
- Door hardware.
- Review of building security management systems including Paxton / Axis / Stanley / Saito / HID etc.

Build review

- Build review of Windows / Linux systems. The possibility to build review other systems after discussion.

CCTV

- Review of Axis / Hikvision / Hilink etc. devices.
- Wireless CCTV jamming.
- Review of VMS systems like Milestone or Avigilon.

Wireless

- 802.11, Bluetooth and bespoke protocols.
- Some knowledge of 4G/5G base station stuff, eNB, SCMA, NR, RAN etc, though would have to talk about the project before accepting.

Embedded devices

- Embedded Linux / Windows / Android and other operating systems.
- Uboot / secure boot attacks.
- Attacking serial, JTAG and other debugging interfaces.
- Key recovery / attacking discrete TPMs.
- Web interface attacks.
- Memory contents extraction.

Protocol analysis

- Analysis and attacks against custom protocols.

Code review

- Secure code review.
- Code assisted assessments.

Kubernetes / containers

- Configuration review
- Local and intra-component attacks using containers and management system.

Cloud

- Salesforce SaaS / PaaS services.
- Oracle SaaS / PaaS services.
- Azure / AWS review of whole deployment or individual services.
- We have some experience with IBM cloud and Huawei cloud.

Cryptography

- General use of cryptography / hardcoded key recovery / advice on secure use of cryptography / chain of trust.

SDLC / Devops

- General organizational / development process maturity level assessment.
- Secure development.
- Secure build chain / software supply chain (if given a little notice as would need to review).

SAP

- Some experience of securing SAP systems.

Threat modelling

- We can produce detailed and high-level threat models.

AI / LLM Assessment

- We can assess LLM systems like chatbots to test data exposure / jailbreaking / offensive behaviour.

Tech QA / blog posts