BULLET PROOF

RED TEAM DATA SHEET

UNRESTRICTED

1. RED TEAM

1.1 SERVICE DESCRIPTION

A Bulletproof Red Team assessment is a comprehensive security audit that attempts to breach your organisation's physical and cyber security defences. Red Teaming is a multi-layered process and our expert operatives will leverage every technical and social engineering weakness in an attempt to compromise your security. This will involve blending vulnerability scanning, penetration testing, social engineering and culminating in a physical breach attempt.

Bulletproof Red Team assessments are as unique as your organisation, with each engagement tailored to meet your specific objectives. This customisation ensures your business will be best placed to shore-up your defences against various methods of real-world attacks, whilst keeping within set budget and time constraints.

1.2 KEY FEATURES

- Challenge your organisation's security assumptions
- Identify and exploit weaknesses in your physical and cyber defences
- Uncover flaws in your security processes
- Multi-layered approach for maximum impact
- A carefully pre-defined scope will set the rules of engagement

1.3 DELIVERABLES

At the end of the project, we will provide a comprehensive yet easy-to-understand report that will detail our activities and the discovered security weaknesses:

- Analysis of system and application vulnerabilities and exploits that were discovered
- A breakdown of physical weaknesses
- Detail on how vulnerable your organisation is to social engineering
- Remediation advice to help you bolster your cyber defences

1.4 METHODOLOGY OVERVIEW

Our testing procedure is in-line with industry best practices and makes use of the CREST framework as an overarching methodology, into which we embedded the PTES and OWASP practices. Any automated tools that we use during the assessment will have all plugins and signatures up-to-date, allowing us to uncover the latest security flaws in your systems.

Bulletproof Red Team Assessments are split into eight distinct stages:

1. **Pre-engagement**
   Accurate scoping to meet your objectives and agreeing commercials

2. **Intelligence gathering**
   Including extensive open-source intelligence and password dumps

3. **Vulnerability analysis**
   Analyse your organisation for exploitable vulnerabilities

4. **Infrastructure exploitation**
   Actively exploit discovered vulnerabilities on your systems

5. **Application exploitation**
   Move up the technology stack to exploit vulnerabilities in your applications

6. **Physical access intrusion**
   Using information from previous phases to attempt to gain physical access

7. **Post-exploitation**
   Gather evidence of our physical and virtual security breach

8. **Reporting**
   A comprehensive yet easy-to-understand report details all our activities

2. ABOUT BULLETPROOF

2.1 IN-HOUSE SECURITY OPERATIONS CENTRE

At Bulletproof, security's in our DNA. Our security services are the best way to remain ahead of hackers, take control of your infrastructure, and protect your business-critical data. A key feature of Bulletproof is our in-house Security Operations Centre (SOC). Based entirely in the UK, it's the command centre of our cybersecurity operations and is staffed 24/7 by trained, experienced security professionals.

2.2 CREDENTIALS

Bulletproof are:

- CREST approved
- Tigerscheme certified
- PCI DSS v3.2 Level 1 Service Provider
- ISO 27001 certified
- ISO 9001 certified

Our staff are:

- CREST certified
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Offensive Security Certified Professional (OSCP)
- Tigerscheme Qualified Security Test Member (QSTM)
- Certified Ethical Hacker (CEH)
- ISO 27001 Implementer
- CCNA and CCNP Security
- Certified EU GDPR Practitioner

BULLET PROOF

T: 01438 532 900 E: contact@bulletproof.co.uk W: www.bulletproof.co.uk