www.srm-solutions.com
03450 21 21 51

INFORMATION SECURITY TESTING & COMPLIANCE

What is a Red Team Engagement?

In the world of information security which is riddled with acronyms, the deceptively simple 'Red Team' may take a little explaining. Breaking down the initial letters of industry terms usually provides a clear indication of the service provided. But the term Red Team has its origins in the US intelligence community and its actual meaning is a little more mysterious. In that context, a Red Team explores alternative futures, challenging an organisation to improve its effectiveness.

In our context, a Red Team provides real-world attack simulations designed to assess and significantly improve the effectiveness of an entire information security programme.

Where a normal penetration test focuses upon identifying and exploiting issues within a specific system/clearly defined scope, the Red Team differs in that it is very much goal/objective orientated. As a result, this allows for a much larger attack surface for the penetration tester to target in an effort to reach the pre-defined goal/objective.

Purpose?

To put your network, applications, people and processes to the ultimate security test, you need to subject yourself to real-world scenarios that are designed to establish how well your defence and response processes measure up. This is achieved through a combination of simulated social engineering (physical and technical), network and application attacks from SRM.

The Solution?

The key difference between a penetration test and Red Team engagement is the extent of scope; thus replicating the wider view an actual attack would have. Whilst a penetration test is often focused upon a key application or system, a Red Team engagement is fully bespoke and often 'goal orientated'. This goal will often be: 'we have this highly sensitive network/piece of data/solution – can you get access to it?'

With the above in mind this will result in several considerations by the Red Team - e.g. Can the data center housing the information be physically accessed? Can a user be manipulated into providing us with access (via phishing, vishing etc.)? Are network attack vectors present which may allow a level of access? Is a combination of these attack vectors required?

As a result, Red Team engagement includes a wide variety of applications, systems, people and physical locations within the scope of testing. Naturally the extent to which the Red Team will operate and engage will be defined by you, but it will take a wider view of potential attack vectors and mirror a persistent attacker.

A Red Team engagement will therefore have free rein in terms of attempting to gain access to the defined goal whilst ensuring a controlled approach.

The Benefits?

The benefits of this approach is that it allows you to validate your protection, monitoring and response solutions or processes. This assists in ensuring your organisation can respond to an emulated 'real-world' attack where varying avenues of approach can be used, rather than a limited focus on a single system.

The ultimate goal is to use offensive techniques to enable you to identify areas for improvement and/or to validate the capability of your response. Even in the event of the objective not being wholly realized a number of recommendations/learning experiences will still be achieved, thus always assisting towards further improvement of your security capabilities.

SRM Testing Solution Matrix:

	Vulnerability Assessment	Penetration Testing	Advanced Penetration Testing	Red Team	Social Engineering
Free Scope Consultation	✓	✓	✓	✓	✓
Final Scope Agreement	Defined with client	Defined with client	Defined with client	Defined with client	Defined with client
Purpose of Service	Security Health Check	Client objective driven	Client objective driven	Client objective driven	Educational
User Targets			✓	✓	✓
Onsite/Internal Testing	✓	✓	✓	✓	
Remote/External Testing	✓	✓	✓	✓	
Vulnerability Scanning & Identification	✓	✓	✓	✓	
Manual Testing		✓	✓	✓	
Vulnerability Exploitation		✓	✓	✓	
Post Exploitation		✓	✓	✓	
Web Application Testing		✓	✓	✓	
Phishing			✓	✓	✓
Vishing and/or Smishing				✓	✓
Open Source Intelligence (OSINT) Report				✓	✓
Wireless Testing			✓	✓	
Physical Intrusion				✓	✓
Drop Box Placement				✓	✓
Regular Updates/Wash-up Meeting	✓	✓	✓	✓	✓
Detailed Report	✓	✓	✓	✓	✓
Report Walkthrough			✓	✓	✓

About SRM

Accredited by the Payment Card Industry Security Standards Council (PCI SSC), SRM is one of only 22 PFI companies in the world and one of the top 3 PFI Companies operating out of the UK throughout Europe, USA and beyond. But primarily we are an Information Security Consultancy specialising within the Payment Card Industry and Cyber Security sectors. We have been a Qualified Security Auditor since the introduction of the PCI Security Standards

SRM - Cyber Security Suppliers to:

HM Government

PCI Security Standards Council
PCI FORENSIC INVESTIGATOR™