



SAFECOMMS

SERVICE BRIEFING: INTERNAL PENETRATION TEST

Objectives

The objective of an Internal penetration test is to ascertain what levels of unauthorised access and malicious activity an authenticated user logged onto the internal network could achieve. (Such a user could be – for example – a disgruntled employee, a “rogue” external contractor, or an employee with criminal tendencies). By conducting this testing, vulnerabilities that could potentially be exploited by an attacker will be identified, and pre-emptive remediation steps can be taken to secure the organisation before an attacker strikes.

Scope

The scope of the testing will generally cover all internal hosts. Whilst the testing will focus mainly on ascertaining what a malicious authenticated user could achieve, the project will typically also include an additional set of testing based on being able to physically plug into the internal network but with no log on credentials.

Methodology

The Safecomms consultant is given physical access to the internal network and a set of “standard” log on credentials for the purposes of the testing. The Safecomms consultant will then use the same tools and techniques that a skilled user with malicious intent would use. The testing will, however, be non destructive and will stop short of exploitation (unless otherwise agreed). Typically the testing methodology will comprise the following steps:

- i. An initial covert intelligence-gathering exercise, where the Safecomms consultant gathers as much information as possible about the internal network, IT infrastructure and supporting IT processes. Safecomms uses a variety of methods and tools to gather this intelligence, including DNS, NMAP, Amap, Ping and Traceroute.
- ii. Based on the intelligence gained in the previous step, Safecomms develops and executes a specific attack plan. Tools and techniques used will typically include

- Netcat
- Nessus
- Nikto
- Metasploit
- Wardialling
- Hand crafted attack scripts
- CVE
- CERT
- Bugtraq
- Brute force tools
- Packet sniffers
- Safecomms proprietary ethical hack tools

Deliverable

The deliverable comprises a report containing the following:

- i. An Executive Summary explaining the key findings of the testing in plain English, written from a risk management perspective and aimed at non technical senior management.
- ii. Detailed findings arising from each vulnerability identified, explaining and classifying the risks associated with each finding.
- iii. Specific detailed recommendations for the smartest and most cost effective remediation steps for each vulnerability.



If a penetration test is to be of any real value, all the tools and techniques that a sophisticated “black hat” hacker would use must be brought into play.

Contact Safecomms

Tel: +44 (0) 1223 576044
Fax: +44 (0) 8708 362157

info@safecomms.co.uk

16 Millers Yard,
Mill Lane,
Cambridge, CB2 1RQ, UK

