digicore

7safe

Penetration Testing

Overview

ISO 27001 BUREAU VERITAS Certification

ISO 9001 BUREAU VERITAS Certification

Penetration Testing

Sometimes referred to as “ethical hacking”, penetration testing is the process of testing computer security by attempting to compromise it.

Digicore and 7Safe’s approach

Our penetration testing team addresses the wide-ranging needs of clients. We offer an in-depth and comprehensive service for systems, from external and internal perspectives.

Security testing involves either conducting tests via the Internet to simulate the view of your systems through the eyes of a potential attacker, or by attending your site and connecting to your internal network. The on-site approach allows our testers to view services and resources from behind the external perimeter to identify vulnerabilities.

Vulnerability Assessments are automated scans in which weaknesses are not actively exploited unless they are considered to be safe.

Penetration Testing actively exploits apparent weaknesses in an attempt to prove that they are points of vulnerability, and to reveal other potential weaknesses.

Application Tests are used to identify and assess potential threats to software applications, including bespoke or proprietary systems.

Social Engineering relies heavily on human interaction and often involves tricking other people into breaking security procedures.

Wireless Security Tests assess the security risks associated with 802.11 (WiFi) wireless networks.

Testing Process

1. **Scoping**
   Assessing the appropriate targets for penetration testing
2. **Discovery**
   Gathering information about a network & its services
3. **Vulnerability scanning**
   Testing systems and services for known vulnerabilities
4. **Target penetration**
   If within testing scope, systems may be compromised
5. **Analysis**
   Analysing the results from previous testing stages
6. **Report**
   A high level management summary, followed by technical findings and recommended corrective actions

Our testing is designed to ensure that systems are operating as expected and to reveal previously hidden or undiscovered security related issues.

Case Studies

Remote test

The client requested that 7Safe conduct a penetration test, including exploitation vulnerabilities discovered on computers in their public facing IP address range.

Analysis of the public facing network revealed that the majority of accessible devices were reasonably well configured; however, two of the devices exhibited high-risk vulnerabilities.

One device contained copies of the Windows Command Interpreter in the /scripts folder. These files acted as a functional back door and could be used to execute a wide range of commands. To illustrate this 7Safe created a folder called C:\7Safe on the server. The fact that these rogue files existed on the server indicated that security had been compromised in the past by an attacker or malicious software (such as a worm).

Result:

7Safe recommended that an investigation be conducted as to how these rogue files came to exist on the server and advised that a complete rebuild of the server from clean media may be required.

Application test

During this assignment, it was found that a client's web server suffered from a SQL Injection flaw. This flaw was caused by poor validation of input accepted by the web server application. The application took the input from the end user and passed it to the backend SQL server without validation. It was also possible for an attacker to login as any user in the database, or worse, to obtain any information contained within the database, including all user transactions, contact details and more.

Result:

7Safe advised the client of the flaws identified. Consequently an in-house programming team was able to address the issues so that they no longer provided a security threat to the organisation.

Wireless test

A client commissioned 7Safe to review their wireless network security. An internal network analysis by 7Safe revealed several vulnerabilities in the clients system; these were predominantly caused by default, ineffective or missing passwords, and also the fact that numerous critical security patches were not installed. The identified weaknesses made it possible for 7Safe consultants to obtain access to sensitive data and information, including passwords for all services on the network.

Both of the wireless networks that 7Safe encountered in their analysis implemented WEP encryption. Unfortunately, weaknesses in the WEP implementation made it possible to execute an attack that revealed the key (password). 7Safe demonstrated this fact and retrieved the key in under an hour. Both wireless networks broadcasted their identifier.

Result:

7Safe recommended that strong passwords be in place for all services and that all devices be properly security hardened, regardless of whether they were public facing or not.

It was also recommended that all devices utilise WPA encryption (preferably coupled with access control mechanisms like 802.1X with PEAP) and that the identifier broadcast be disabled.

7safe

digicore

information security services

Penetration Testing Education

Masters-level training and certification in penetration testing is also provided by Digicore. This includes the Certified Security Testing Associate (CSTA) and Certified Security Testing Professional (CSTP), which form part of the world's first Postgraduate Certificate in Penetration Testing and Information Security.

- PCI DSS
- ISO 27001 Consulting
- Computer Forensics
- Penetration Testing
- Education

t +353 1 6854 942

w www.digicore.ie