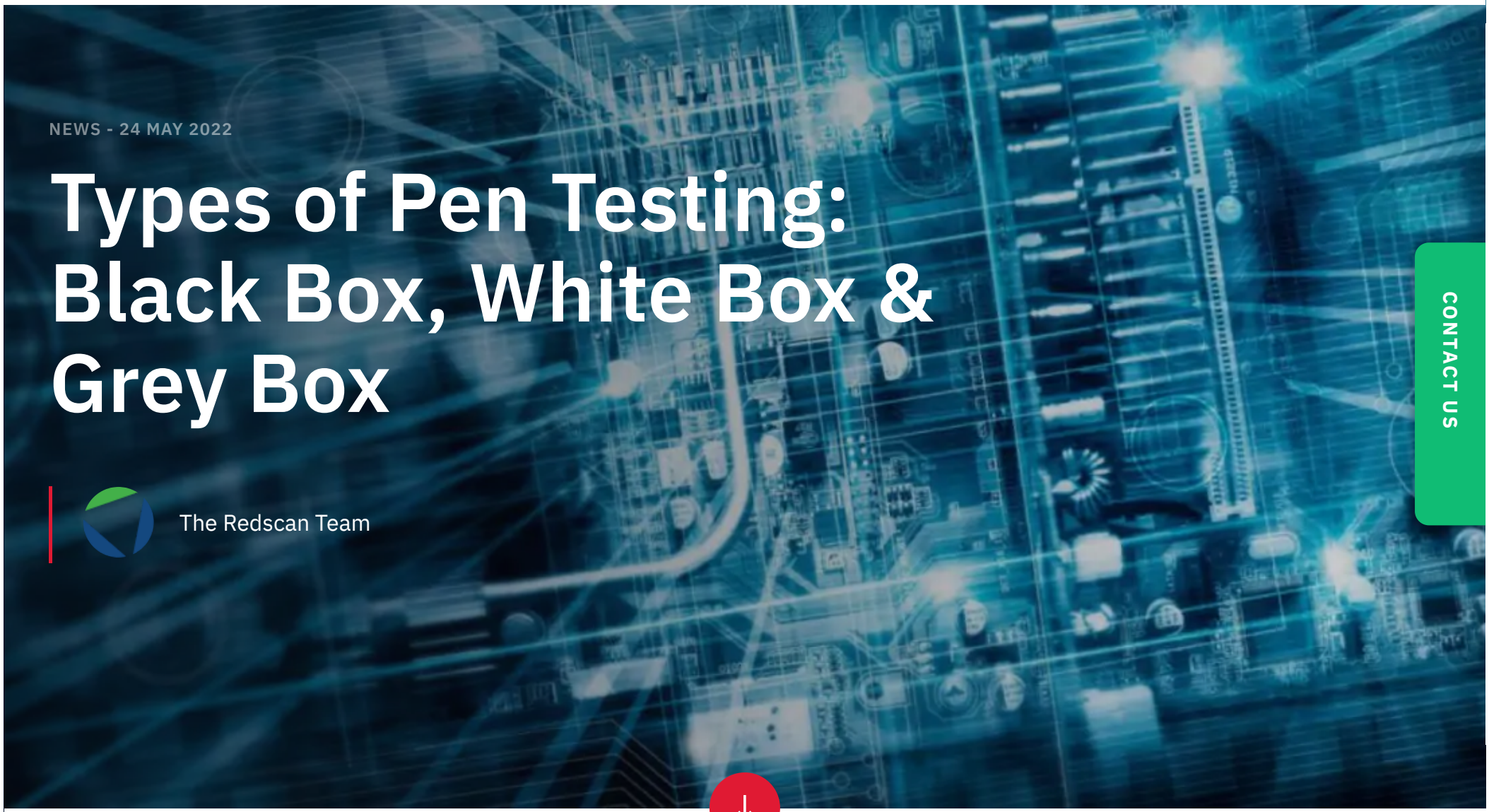

NEWS - 24 MAY 2022

Types of Pen Testing: Black Box, White Box & Grey Box

The Redscan Team

Last updated on **July 26, 2022 at 13:35 PM**

With so many types of penetration testing on offer, it can be difficult to ascertain which assessment meets the needs of your business.

This blog attempts to cut through the industry jargon to provide all the information you need to identify the right pen test for your organisation, including the important question of whether you require a black box, white box or grey box testing style.

What is pentesting?

A pen test is a form of ethical cyber security assessment conducted to identify, safely exploit and help eliminate vulnerabilities that reside across an organisation's on-premises and remote IT environments.

It is recommended that all organisations commission security testing at least once per year, with additional assessments following significant changes to infrastructure, as well as prior to product launches, mergers or acquisitions. Organisations with very large IT estates, who process significant volumes of personal and financial data or have strict compliance requirements to adhere to, should conduct pen tests with a higher frequency.

Before selecting a suitable provider, it's important to be familiar with the types of pen test available, as engagements vary in focus, depth and duration. Common ethical hacking engagements include:

1. Internal/External Infrastructure Penetration Testing

An assessment of on-premise and cloud network infrastructure, including firewalls, system hosts and devices such as routers and switches. Can be framed as either an internal penetration test, focusing on assets inside the corporate network, or an external penetration test, targeting internet-facing infrastructure. To scope a test, you will need to know the number of internal and external IPs to be tested, network subnet size and number of sites.

2. Wireless Penetration Testing

A test that specifically targets an organisation's WLAN (wireless local area network), as well as wireless protocols including Bluetooth, ZigBee and Z-Wave. Helps to identify rogue access points, weaknesses in encryption and WPA vulnerabilities. To scope an engagement, testers will need to know the number of wireless and guest networks, locations and unique SSIDs to be assessed.

3. Web Application Testing

An assessment of websites and custom applications delivered over the web, looking to uncover coding, design and development flaws that could be maliciously exploited. Before approaching a testing provider, it's important to ascertain the number of apps that need testing, as well as the number of static pages, dynamic pages and input fields to be assessed.

4. Mobile Application Testing

5. **Build and Configuration Review**

Review of network builds and configurations to identify misconfigurations across web and app servers, routers and firewalls. The number of builds, operating systems and application servers to be reviewed during testing is crucial information to help scope this type of engagement.

6. **Social Engineering**

An assessment of the ability of your systems and personnel to detect and respond to email phishing attacks. Gain precise insight into the potential risks through customised phishing, spear phishing and Business Email Compromise (BEC) attacks.

GET A PEN TEST QUOTE TODAY →

White box vs black box vs grey box pen testing

The amount of information shared prior to an engagement can have a huge influence on its outcomes. Testing style is usually defined as either white box, black box or grey box penetration testing.

White box penetration testing

White box penetration testing, sometimes referred to as crystal or oblique box pen testing, involves

Black box penetration testing

In a black box penetration test, no information is provided to the tester at all. The pen tester in this instance follows the approach of an unprivileged attacker, from initial access and execution through to exploitation. This scenario can be seen as the most authentic, demonstrating how an adversary with no inside knowledge would target and compromise an organisation. However, this typically makes it the costliest option too.

Grey box penetration testing

In a grey box penetration test, also known as a translucent box test, only limited information is shared with the tester. Usually this takes the form of login credentials. Grey box testing is useful to help understand the level of access a privileged user could gain and the potential damage they could cause. Grey box tests strike a balance between depth and efficiency and can be used to simulate either an insider threat or an attack that has breached the network perimeter.

In most real-world attacks, a persistent adversary will conduct reconnaissance on the target environment, giving them similar knowledge to an insider. Grey box testing is often favoured by customers as the best balance between efficiency and authenticity, stripping out the potentially time-consuming reconnaissance phase.

Choosing the right pen test provider

When commissioning a pentest, it's important to ensure the company has the necessary expertise to not only detect a wide range of vulnerabilities, but also provide the assistance you need to remediate