The Cyber Source blog

Cyber Security, in plain English

DECEMBER 4, 2018

TYPES OF PENETRATION TEST - WHAT'S THE DIFFERENCE?

By Comtact Cyber Security, Penetration Test

Penetration testing has become a vital part of a modern vulnerability management programme. Just like in today's Hollywood thrillers, industrialised hackers around the world are trying to breach network defences - not just of national banks, Government organisations, or big corporate brands, but also of any company - of all sizes - with easily discovered and exploited security vulnerabilities.

> Hacking is now industrialised

Recent Posts

Threat Intel December 2019: 36 vulnerabilities including 7 critical

steps required to fix them (before they are exploited for real).

[The Ultimate Handbook to Penetration Testing] - Procure, plan and manage the life cycle of a penetration testing project »

But there are several different types of pen test, each with a different viewpoint, and objective so it is important to know the differences - so you know which type of test meets your requirements and objectives.

What are the different types of Pen Test?

While there are numerous sub-categories and variations, generally, the different types of penetration test can be divided into four main groups. Let's take a look:

1. External network penetration test

An external pen test involves an ethical hacker trying to break into an organisation's network - across the Internet. This means it's done off-site (remotely, as a hacker would be), using controlled and agreed ethical hacking techniques to accurately simulate a targeted attack from malicious parties on your network.

Benefits of a network pen test

An external pen test probes your perimeter defences, providing an effective test of how your externally-facing network infrastructure responds to threats, and where potential weaknesses and vulnerabilities lie.

Network devices, servers and software packages represent a constant challenge to secure, and a frequent opportunity for attack. Network penetration testing allows you to find your most exposed security vulnerabilities before they can be exploited.

As with all pen testing methodologies, a hacker will perform an intelligence-gathering phase from publicly available sources to identify opportunities and vulnerabilities to exploit. This would include using performing a vulnerability scan to identify potential weaknesses to exploit, e.g. misconfigurations, weak passwords, unpatched software, open ports etc.

2. Internal network penetration test

An internal penetration test, by contrast, simulates either the actions a hacker might take once access has been gained to a network, or those of a malicious actor, or disgruntled employee

penetration test (above), but the starting point assumes a degree of network access already.

Why perform an internal pen test?

An internal network pen test is typically performed from the perspective of both an authenticated and non-authenticated user to ensure that the network is critically assessed for both the potential exploit of a rogue internal user, and an unauthorised attack.

Naturally, with GDPR in mind, you will also be checking the potential for users to access and leak any confidential, sensitive or personally identifiable information (PII).

3. Web application penetration test

The number of web apps and websites is growing rapidly, many providing easy access to sensitive user or financial data, making them a highly prized target for cybercriminals.

websites and web applications, including CRM, extranets and internally developed programmes - which could lead to exposure of personal data, credit card information etc.

Increased demand for web application pen testing

From web-based portals to online shopping and banking, today organisations are building their businesses directly online. As these systems grow increasingly powerful, they also scale in complexity, meaning the range of exploitable vulnerabilities is rising.

Internet-based web applications are in their nature, globally accessible and easily probed, or manipulated – from anywhere, at any time – creating some of the most pressing issues facing any organisation.

4. Social Engineering

Social engineering is commonly seen as the modern frontier in IT security - and certainly your greatest risk. Your users.

> A social engineering pen test will help you assess and understand the susceptibility within your organisation to human manipulation via email, phone, media drops, physical access, social media mining etc.

What is Social Engineering?

Social engineering techniques are wide ranging, from the very

By manipulating those closest to the target - your employees - these attackers use simple, but highly effective psychological tactics to lure your employees into granting privileged network access, or sending a sensitive file, or paying a supposedly urgent invoice.

Rather than finding exotic backdoor vulnerabilities and resorting to high-tech tools and strategies, social engineering attacks organisations through their own front door.

Benefits of a social engineering Pen Test

In practice, hackers (and ethical hackers) will often use social engineering tactics as a first step, to gain a foothold into the network, from which they can elevate user privileges - it is often easier to exploit users' weaknesses than it is to find a network or software vulnerability.

Social engineering pen testing can reveal a lot about the cyber security awareness levels of your employees, and their level of compliance with existing security policies in place.

Which type of pen test is right for me?

So there it is: we've gone through the four main types of penetration tests - all providing a rigorous 'real-world' test of your existing security controls.

But importantly, an individual pen test should be tailored to meet your objectives - as there is no 'one size fits all' - following different strategies and methodologies to identify possible points of weaknesses and compromise.

Detailed risk-based report

Once completed, you should expect an 'easy to understand' risk-based report, suitable for both technical & non-technical staff, with details of the steps taken pen tester to breach the network/defences - plus the necessary remediation or next steps.

View a free sample Pen Test report

Take a look at a sample risk-based report to understand the approach, critical security intelligence and actionable steps with our CREST-certified penetration tests.

Further reading

- Questions to ask your pen test provider

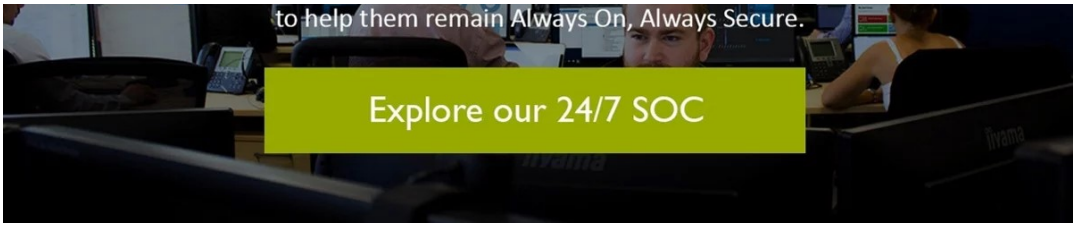
- 6 steps to a successful cyber security improvement programme
- The difference between a Vulnerability Scan and a Penetration test
- Pros and cons of outsourcing your Cyber Security - In-house, MSSP, or Virtual SOC?

About Comtact Ltd.

Comtact Ltd. is a government-approved Cyber Security and IT Managed Service Provider, supporting clients 24/7 from our ISO27001-accredited UK Security Operations Centre (SOC).

Located at the heart of a high security, controlled-access Tier 3 data centre, Comtact's state-of-the-art UK Cyber Defence Centre (SOC) targets, hunts & disrupts hacker behaviour, as part of a multi-layered security defence, to help secure some of the UK's leading organisations.

03452 75 75
75



SHARE THIS STORY | |

NEXT POST →

Contact us: **03452 75 75 75**

UK Security Operations Centre

Our Team

Locations

Comtact Ltd. (Central)

As our SOC / NOC is located within a high security Tier 3 data centre, location is protected.

Comtact Ltd. (London)

SOC Services

- Security Operations Centre
- Penetration Testing
- Vulnerability Management
- Phishing-as-a-Service & Security Awareness Training
- Cyber Essentials PLUS certification

Company

- About Us
- Blog
- Contact Us
- Terms & Conditions
- Privacy Policy
- GDPR Statement

03452 75 75
75

Comtact Ltd. (North)

31-33 Albion Street, Hanley, Stoke-on-Trent ST1 1QF

Services

- 24/7 NOC Services
- 24/7 IT Service Desk
- White Label NOC Services for MSPs
- IT Infrastructure Management
- IT Network Monitoring
- SolarWinds-as-a-Service
- Cloud Migration Services

Accreditations & Awards