netitude

How to Conduct a Penetration Test

SCROLL FOR MORE INFO

1

Planning & Scoping

The first phase starts with planning your pen test by defining objectives and determining the scope of your test (which assets are included in the pen test, etc.). Secondly, whoever is carrying out the penetration test—whether that's your in-house security team or an outsourced Managed Service Provider (MSP)—like us at Netitude—must obtain the necessary permissions and legal approvals before proceeding.

SCROLL FOR MORE INFO

2 Information Gathering

The second step of your penetration test will involve collecting data about your organisation's structure, IP addresses, domains, and services. You could also go the extra mile by taking advantage of Open-Source Intelligence (OSINT) – gathering and analysing publicly available information from various sources (social media, search engines, public records) to gain a more rounded view of cyber attack techniques and strategies.

SCROLL FOR MORE INFO

3 Vulnerability Assessment

Conducting a vulnerability assessment is critical in identifying weaknesses in your existing IT systems. In the initial assessment, assets (devices or systems) should be identified and assessed regarding their importance and value. During this phase, it would also be beneficial to understand the risk factors associated with each asset and the risk appetite, mitigation practices, and business impact of each device. A comprehensive vulnerability assessment should also reveal who can access the devices (admins/senior leadership etc).

SCROLL FOR MORE INFO

4 Exploitation

In the next stage, you'll get to grips with the nitty-gritty of the pen test. This will involve getting your hands dirty by carrying out ethical hacking on your existing IT systems to try and exploit any vulnerabilities that crop up. During exploitation, penetration testers should also evaluate the effectiveness of security-related controls and measures while remaining undetected.

SCROLL FOR MORE INFO

Final Analysis and Review

In the penultimate phase, pen testers should take stock of all the findings they took from the penetration test. We recommend that you carry out the following steps to ensure you cover all bases regarding your penetration test's final analysis and review.

- **Evaluate Findings:** Review the results of the penetration test.
- **Risk Assessment**: Assess the impact and likelihood of exploitation.
- **Recommendations**: Provide actionable recommendations to address vulnerabilities.

SCROLL FOR MORE INFO

6 Reporting

Last but by no means least, it’s time to create a comprehensive report that encapsulates the entire process from start to finish. Here, it would be a good idea to document all findings, including any vulnerabilities and risk levels encountered at each stage.

In the reporting stage, we recommend creating a detailed remediation plan to address the identified vulnerabilities and setting deadlines against each weakness. You can then present an executive summary (concise view of the pen test results) to the organisation’s leadership team that summarises the most critical vulnerabilities discovered during the test that need addressing.

SCROLL FOR MORE INFO

netitude

Did You Find This Guide Helpful?

GET IN TOUCH WITH OUR TEAM OF EXPERTS FOR MORE TECH TIPS

0333 241 2323

hello@netitude.co.uk