Network Penetration Testing Process

1. Reconnaissance:

This step involves active and passive information gathering on the target infrastructure. Tools like *Shodan, Censys, Google, Maltego* (and its various plug-ins) and *NMAP* are used for discovering the interconnected systems (E.g.: Top-Level Domains, sub-domains, IP blocks, internet-exposed systems, and services). This step provides information about systems that are in connection with the target application (a.k.a. “the attack surface”) and enables a holistic approach to security testing. Discovery of the attack surface can also reveal low-hanging fruits - potential "initial entry points" into the internal network or a direct path to exploiting critical information assets, which might not be identified only with the testing of the mobile and web applications.

2. Vulnerability Scans for the Backend Components

Nessus Professional is used for vulnerability scans of the identified systems and services. Identified vulnerabilities will be analyzed both for direct exploitation and for scenarios in which multiple vulnerabilities are chained to construct a high-impact attack.

3. Shortlisted Web Applications

Reconnaissance steps may reveal weak web applications, such as applications that use very old technologies, dormant (forgotten, unused) web applications and test instances. Such applications will be subjected to an audit with a separate checklist that only contains checks aimed at obtaining a foothold into the internal network. In case we foresee that an extensive effort could be required for this activity, prior approval of the client will be sought.

4. Reporting

All high-risk issues identified during the penetration tests are reported to the client within 24 hours. Lower-risk issues are reported at the end of the audit. Issues that are rectified by the client during the fieldwork are verified (re-tested) in a reasonable time frame. Verified issues are dropped from the final report.

A full report is prepared and submitted at the end of the fieldwork, marked as a “pre-rectification version”.

When the rectification is completed, we will check and verify whether the rectifications adequately address the reported vulnerabilities. Completely rectified findings are then dropped from the report.

If rectification for a specific finding is partial in terms of addressing the reported risks, then instead of dropping the finding, we may change (downgrade) the severity rating of the finding instead.

A second full report will be issued after the verification round, which will be marked as the “final version”.