TJTSec

Security Services for SMBs

Penetration Testing

Penetration Testing is designed to test the effectiveness of an organization's overall security. By simulating a real-world attack, weaknesses are identified and remediation steps can be taken to defend against adversaries and increase the organization's security posture.

TJTSec Penetration Testing evaluates the security of:

- Public-Facing Services
- Internal Servers & Workstations
- Wireless Networks
- User Access Level Permissions
- Passwords
- Remote Access
- Routers/Firewalls/Switches
- Wired Networks
- Networked Devices (printers, scanners, faxes, etc.)
- 3rd-party Cloud Services (when authorized by provider)
- Physical Controls (locks, cameras, fencing, etc.)

Deliverable: Upon completion of testing a clear and detailed report is produced which includes a summary of steps taken to infiltrate company systems, missing/ineffective controls, action-items to secure the organization arranged in a timeline based on severity, and technical data to assist with remediation. The engagement is concluded by meeting with stakeholders to discuss findings and answer any questions.

TJTSec
4700 Falls of Neuse Road, Suite 400
Raleigh, NC 27609

919-571-7055
www.tjtsec.com
info@tjtsec.com

TJTSec

Security Services for SMBs

The following is an overview of the Penetration Testing process:

Testing begins by conducting research on the organization through public-resources such as web searches. Information collected includes physical locations, web services (such as public web sites and other Internet-accessible services), contact information for key people, etc. Penetration testing is performed from multiple angles: against public-facing servers via the Internet and against internal systems from within the network.

Via the Internet: After reconnaissance has been completed, in-depth scans are performed against servers identified in the research process to determine exactly what software is exposed to the outside world. Using a combination of open-source and proprietary hacking tools, attacks are carried out on these systems, attempting to gain unintended access to the servers. If access is obtained, entry to the internal network is attempted using a technique referred to as "pivoting".

Via the Internal Network: Scans are conducted against the internal network either through pivoting, as mentioned previously, or by setting up a system on the internal network which mimics a compromised workstation. After enumerating systems and services hosted on the network, access to servers and other workstations is attempted using technical exploits. This may also involve network devices such as scanners, printers, routers, etc. Once entry to other internal systems is achieved, privilege escalation is performed (attempting to gain increased access to systems). This includes administrator permissions, data access, etc. Methods may include password cracking and other technical exploits.

TJTSec
4700 Falls of Neuse Road, Suite 400
Raleigh, NC 27609

919-571-7055
www.tjtsec.com
info@tjtsec.com