1 Penetration Testing

Der Penetration-Test leitet sich vom englischen 'Penetration' ab, was so viel wie ‚Eindringen' bedeutet. Es geht also ums Testen, wie leicht man in Ihr EDV-System eindringen kann.

1.1 Externer Test

- Test der Firewall von aussen auf offene Ports und Schwachstellen. Die IP-Adresse muss bekannt sein oder bei einem vorgängigen Test ermittelt worden sein.
- Test Wireless Lan auf Schwachstellen sowie Passwortstärke und Rogue Access (klassischer Man in the Middle Angriff)
- Überprüfung des Physisches Zugangs ins Gebäude z.B. Scan des Badge (RFID) oder biometrische Zugangskontrollen.

1.2 Interner Test

Im ersten Schritt werden alle auffindbaren Netzwerkgeräte ermittelt. Mittels einem professionellen und aktuellem Schwachstellenscanner werden daraufhin im Idealfall alle Netzwerkgeräte auf Schwachstellen gescannt. Aus Kostengründen kann auch eine beliebige Auswahl an Computern, Servern, Drucker und so weiter vorgenommen werden, um stichprobenweise auf Schwachstellen zu überprüfen.

Beispiel eines Windows XP Computers

192.168.1.244

Summary

Critical	High	Medium	Low	Info	Total
11	2	3	2	20	38

Details

Severity	Plugin Id	Name
Critical (10.0)	11808	MS03-026: Microsoft RPC Interface Buffer Overrun (823980) (uncredentialed check)
Critical (10.0)	11835	MS03-039: Microsoft RPC Interface Buffer Overrun (824146) (uncredentialed check)
Critical (10.0)	12054	MS04-007: ASN.1 Vulnerability Could Allow Code Execution (828028) (uncredentialed check) (NTLM)
Critical (10.0)	12209	MS04-011: Security Update for Microsoft Windows (835732) (uncredentialed check)
Critical (10.0)	13852	MS04-022: Microsoft Windows Task Scheduler Remote Overflow (841873) (uncredentialed check)
Critical (10.0)	18502	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896422) (uncredentialed check)
Critical (10.0)	21655	MS04-012: Cumulative Update for Microsoft RPC/DCOM (828741) (uncredentialed check)
Critical (10.0)	22194	MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)
Critical (10.0)	34477	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)
Critical (10.0)	35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)
Critical (10.0)	73182	Microsoft Windows XP Unsupported Installation Detection
High (7.5)	11110	MS02-045: Microsoft Windows SMB Protocol SMB_COM_TRANSACTION Packet Remote Overflow DoS (326830) (uncredentialed check)
High (7.5)	22034	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)
Medium (5.0)	16337	MS05-007: Vulnerability in Windows Could Allow Information Disclosure (888302) (uncredentialed check)
Medium (5.0)	26920	Microsoft Windows SMB NULL Session Authentication
Medium (5.0)	57608	SMB Signing Required
Low (3.3)	11197	Multiple Ethernet Driver Frame Padding Information Disclosure (Etherleak)
Low (2.6)	42263	Unencrypted Telnet Server
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

Die Untersuchung ergab 11 kritische, 2 hohe und 3 mittlere Sicherheitsprobleme

1.3 Website Security

Webseiten sind natürlich frei aus dem Internet erreichbar. Damit sind sie aber auch einem erhöhten Risiko ausgesetzt. Webseiten können gehackt werden und so für politische Statements missbraucht werden (Webseiten-Verunstaltung) oder mit Trojanern verseucht werden. Zu den Untersuchungen der Website gehören die folgenden Themen:

- Analyse Webserver mittels Fingerprinting (WhoIs) und Google Hacking (Google Suchoperatoren). Wichtig sind auch Informationen zum Webserver und dem CMS wie z.B. WordPress.
- Port und Vulnerability Scanning mittels diversen Tools.
- OWASP (Open Web Application Security Project) Top 10