Pen-Test Standard

Der Penetration-Test (kurz Pen-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. Im Standard-Test wird dazu die Hard- und Software auf Schwachstellen untersucht. Mittels professioneller Software werden die einzelnen PCs, Server und Peripherie auf Herz und Nieren geprüft. Zusätzlich erfolgt eine Überprüfung des Netzwerkverkehrs auf verdächtige Aktivitäten.
Nebst einer Präsentation der Resultate wird ein detailliertes Protokoll erstellt und Lösungen zur Beseitigung der Sicherheitsmängel vorgeschlagen.

Vulnerability Scanning

Im normalen Scanning 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

Hegner Engineering • **Solutions for IT security • against Cybercrime**
Aeussere Bahnhofstr. 30c • CH-8854 Siebnen • T +41 55 440 74 18 • M +41 78 600 68 99
info@hegner-engineering.ch • www.hegner-engineering.ch

Beispiel eines Linux Servers

192.168.6.60

Summary

Critical	High	Medium	Low	Info	Total
0	0	2	2	30	34

Details

Severity	Plugin Id	Name
Medium (5.0)	26919	Microsoft Windows SMB Guest Account Local User Access
Medium (5.0)	57608	SMB Signing Required
Low (2.6)	70658	SSH Server CBC Mode Ciphers Enabled
Low (2.6)	71049	SSH Weak MAC Algorithms Enabled
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10223	RPC portmapper Service Detection
Info	10267	SSH Server Type and Version Information
Info	10273	Samba Web Administration Tool (SWAT) Detection
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10395	Microsoft Windows SMB Shares Enumeration
Info	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
Info	10860	SMB Use Host SID to Enumerate Local Users
Info	10881	SSH Protocol Versions Supported
Info	11011	Microsoft Windows SMB Service Detection
Info	11111	RPC Services Enumeration
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	17651	Microsoft Windows SMB : Obtains the Password Policy
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	25220	TCP/IP Timestamps Supported

4

Die Untersuchung ergab keine kritische und hohe Bedrohung, sondern nur 2 mittlere Sicherheitsprobleme.

Organisation

Nach Absprache mit dem EDV-Verantwortlichen braucht es Zugriff aufs Netzwerk. Die Netzwerkgeräte sollten natürlich eingeschaltet und im Netzwerk erreichbar sowie eingeloggt sein. Bei wichtigen Komponenten wie Server sollte die Überprüfung ausserhalb der normalen Betriebszeiten erfolgen.
Bei einer fehlenden Dokumentation der Netzwerktopologie braucht es ein umfangreiches Scanning, um alle Netzwerkgeräte zu finden.
Zur Analyse des Netzwerkverkehrs mittels Wireshark oder Snort braucht es ein Port Mirroring auf den Internetzugang. Für einen professionellen Switch ist dies problemlos lösbar.
Bei Windows-PCs lässt sich mittels Admin-Freigabe auch die Software auf Schwachstellen untersuchen.