Penetrationstest fürs LAN

1. Durchführung des Tests

- am besten von externen Dienstleistern für objektive Bewertung und zum Ausgleich fehlenden Know-hows
- Überprüfung in regelmäßigen Abständen (neue Dienste, Änderungen am Netz)
- externer Test: Angriffsflächen über das Internet (Dienste wie Mail, http)
- interner Test: Sicherheit einzelner Systeme und der Netzwerkkomponenten

2. Footprinting – Beschaffung von Informationen über das Zielobjekt

- whois-Datenbanken: http://www.ripe.de, http://whois.arin.net
  Ermitteln von Domaininhabern, deren Mailadresse, Telefonnummern, usw.
- Untersuchung der Webseite des Unternehmens nach Infos und Scriptfehlern
- Nutzung dieser Daten für Social Engineering und Phishing-Attacken

3. Scanning – das Netz aktiv überprüfen

- vom Portscan (nmap) bis zu komplexen Security-Scannern (LANGuard)
- komplette Portliste unter www.iana.org/assignments/port-numbers
- Banner-Grabbing des Dienstes (am einfachsten mit Telnet, besser sind Superscan oder Amap)
- Umgehen von IDS-Systemen mit Timing (nmap –T) und SYN-Stealth-Scan (nmap –sS)
- Identifizierung des Betriebssystems (nmap –O)
- mit traceroute, nslookup und finger die Netztopologie aufdecken (einfacher mit Sam Spade)
- für externen Test eher ungeeignet, da durch Firewall geblockt

4. Enumeration – der Angriff beginnt

- geprüft werden sollten Testrechner mit der gleichen Konfiguration wie der echte Server (DOS-Attacken)

externer Test

- Brute-Force-Angriffe gegen unsichere Passwörter
- Einsatz von local (man muss eingelockt sein) und remote Exploits (www.securiteam.com oder www.securityfocus.com)
- bei nicht vorhandener DMZ reicht der Hack des Routers (offner Remotezugang nach außen über Ports 23, 80 oder 256 bei Cisco-Routern) mit Standardpasswörtern der Hersteller (www.cirt.net/cgi-bin/passwd.pl)
- Einsatz von Vulnerability-Scannern gegen erkannte Dienste auf Fehlkonfiguration, Skripte, Bugs (z. B. Nikto)
- Wardialing: Modemscan des Telefonnummernblocks gegen Remote-Access-Zugänge (Phone-Sweep, das kostenlose THC-Scan)

interner Test

- Sniffen von Arp-Paketen zum Aufdecken aktiver Hosts und der Adressbereiche
- Hosterkennung mit Ping-Sweep nicht bei personal Firewalls (nmap –sP 192.168.1.0/24)
- Einsatz von Security-Scannern zur Identifizierung von Diensten, Patchlevel, Paswortsicherheit, …
  Achtung: die gefährlichen neuen Sicherheitslücken werden nicht erkannt!
- Erkennen von Netzwerkfreigaben mit Brute-Force-Angriff (Tool: Shares Finder)
- Angriff der Switche mit einem ARP-Storm (Ettercap)