iMes IT-Penetrationstest

IT-Sicherheitsaudit und Sicherheitsanalyse

Simulierte Eindringversuche in Computernetzwerke – die sieben Phasen des iMes IT-Penetrationstests

Es ist sinnvoll den **IT-Penetrationstests** in verschiedene Gruppen einzuteilen. Man kann zwischen sog. **Black-Box**-Penetrationstests und **White-Box**-Penetrationstests unterscheiden.
Bei einem **Black-Box**-Test ist das zu testende System unbekannt. Der Tester weiß nicht, auf welches System er trifft.
Bei den **White-Box**-Tests sind Betriebssystem, laufende Dienste und weitere Interne bekannt .

Es kann das komplette IT-Netzwerk des Unternehmens oder auch einzelne Bereiche wie **WLAN**- oder **VPN**-Anbindung einem Penetrationstest unterzogen werden.

Der eigentliche **Penetrationstest** lässt sich in **sieben Phasen** gliedern, wobei Phase zwei und vier mehrmals zyklisch durchlaufen werden.

Der **iMes Penetrations-test** stellt einen simulierten Eindring-versuch in Computer-netzwerke dar – der **iMes Penetrationstest** deckt Sicherheitslücken und Schwachstellen auf und garantiert so die nachhaltige Sicherheit Ihrer Systeme und Netzwerke.

Erste Phase:

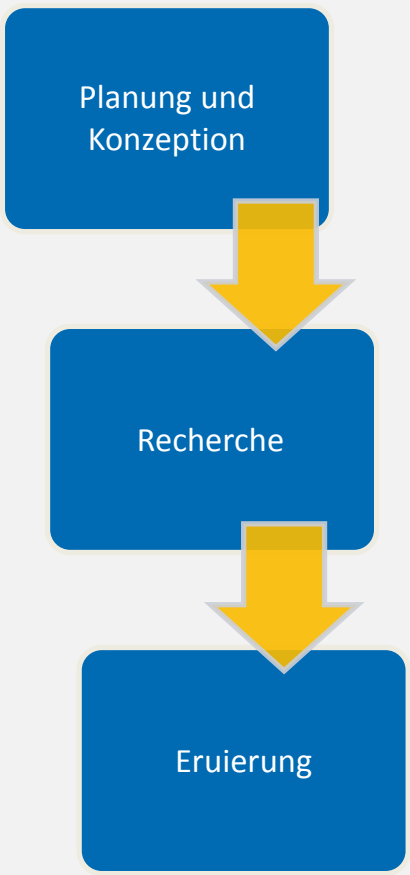
- Erwartungen werden geklärt und Ziele festgelegt
- Fixieren von Eskalationsstufen für den Notfall
- Festlegung von Ansprechpartnern
- Klassifizierung der Sicherheitsanalyse
- Bestimmung des Testzeitraums

Zweite Phase:

- Recherche über das Zielsystem in…
  - Offenen Datenbanken für DNS-Einträge
  - Newsgruppen
  - Web-Foren
  - etc.

Dritte Phase:

- Betriebssystem des Rechners und angebotene Dienste werden eruiert
- Zu überprüfenden Rechnersysteme werden einem sog. **Portscann** unterzogen
  - offene Ports lassen Rückschlüsse auf die zugeordneten Anwendungen zu
- **Fingerprinting**
  - Name und Version von Betriebssystemen und Anwendungen werden in Erfahrung gebracht



prozessleitsystemunabhängig - skalierbar - intuitiv

iMes IT-Penetrationstest

IT-Sicherheitsaudit und Sicherheitsanalyse

Simulierte Eindringversuche in Computernetzwerke – die sieben Phasen des iMes IT-Penetrationstests

- Teilweiser Einsatz von **Schwachstellenscannern**
  - **ABER:** kein Ersatz für das manuelle Vorgehen
- als Abschluss von Phase vier erfolgt eine erste Bewertung des Zielsystems
- Erste Aufwandsschätzung für unautorisierte Zugriffe auf Computersysteme und Netzwerke

Vierte Phase:

- **Schwachstellenrecherche**
  - zielgerichtete Suche nach Schwachstellen in Betriebssystemen und Anwendungen
  - wenn verfügbar: **Exploit** (Programm zur Ausnutzung der Schwachstellen

Fünfte Phase:

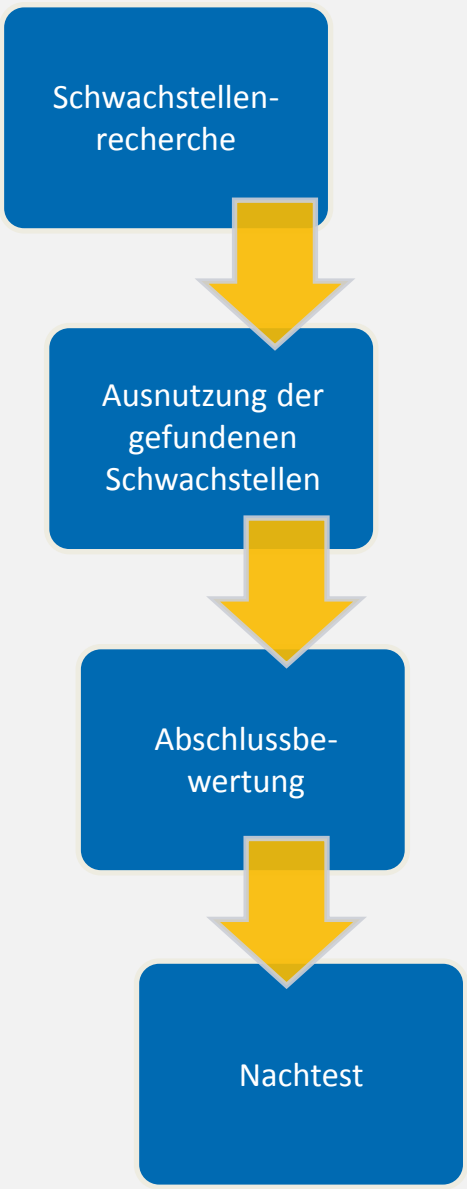
- Ausnutzung der aufgedeckten Sicherheitslücken
  - **ZWECK**: Zugriff auf das System bzw. Vorbereitung weiterer Angriffe
  - Gezielte Angriffe auf Rechnersysteme

Sechste Phase:

- **Abschlussbewertung**
- Erstellung des Abschlussberichts und einer Managementzusammenfassung:
  - Prüfungsauftrag, Prüfungsergebnisse
  - Empfohlene Vorgehensweise
  - Logfiles, Einsatzzeiten (welcher Angriff wurde zu welcher Zeit durchgeführt)

Siebte Phase:

- Durchführung eines Nachtests etwa 30 Tage nach dem Penetrationstest
- Wirksamkeit der Sicherungsmaßnahmen wird überprüft



prozessleitsystemunabhängig - skalierbar - intuitiv