Krisen, KRITIS & Datenschutz

CAMPUS TAGE

www.campustage.org

dsn Aka demie

---

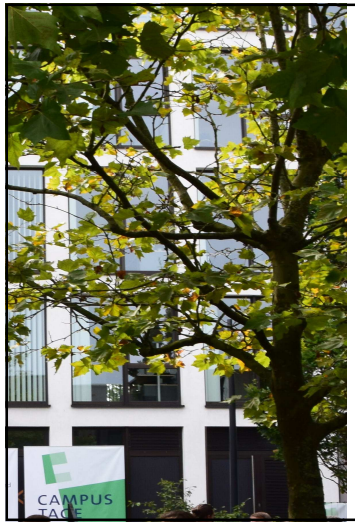
dsn Aka demie

Pentests

Häufige Missverständnisse und sinnvolle Anwendungsbeispiele

CAMPUSTAGE 2023

www.dsn-group.de



dsn Aka demie

Christopher Reusche
Berater Informationssicherheit | Penetrationstests

datenschutz nord Gruppe
T +49(0)421 69 66 32 341
E-Mail creusche@datenschutz-nord.de

www.dsn-group.de

Agenda

dsn Aka demie

Was ist ein Pentest?

Beispiele

Unklarheiten & Missverständnisse

1. Was ist ein Pentest?

Einordnung und Abgrenzung

Was ist ein Pentest?

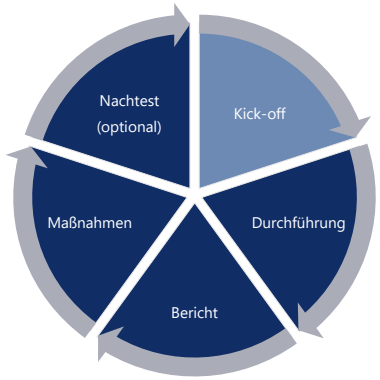
- Testgegenstand
- Zeitraum
- Pentester:in

Was ist ein Pentest?

- Werkzeug in der Informationssicherheit
- Eingeschränkter, simulierter Angriff auf Testgegenstand
- Ziel: Schwachstellen und Verbesserungspotentiale aufdecken
- Automatisierte Tools
- Manuelle und weiterführende Testmethoden
- Individualisiertes Testverfahren

Was ist ein Pentest?

- Testgegenstand und Scope
- Black-, Grey-, oder White-Box
- Individuelle Absprachen



Was ist ein Pentest?

- Informationsgewinnung
- Automatische Scans
- Manuelle Testmethoden

Was ist ein Pentest?

- Management Summary
- Identifizierte Schwachstellen
- Handlungsempfehlungen

Was ist ein Pentest?

- Analyse der Ergebnisse
- Nachbesprechung (optional)
- Behebung von Schwachstellen

Was ist ein Pentest?

- Überprüfung von Maßnahmen
- Ggf. bestimmter Fokus
- Aktualisierter Bericht

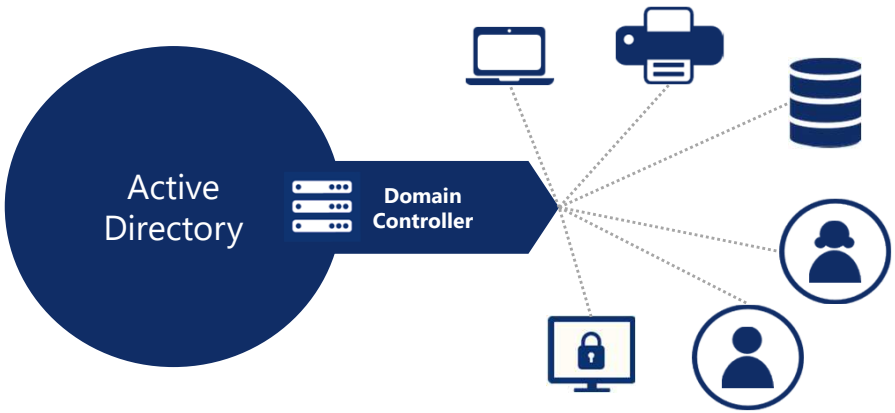
Abgrenzung: Security Scans

- Auswertung erfordert häufig Fachkenntnisse
- False Positives
- Preiswerter
- Schnelle Ergebnisse
- (Qualität der) Ergebnisse abhängig vom Prüfobjekt und Scanner
- Monitoring-Methode mit Fokus auf Sicherheit

Abgrenzung: Red Teaming

- Festlegung von konkretem Ziel (z.B. Übernahme des *Domain Controllers*)
- Ähnliche Methoden, Tools, Strategien…
- Ergänzt durch Social Engineering
- Längerer Zeitraum der Durchführung
- Überprüfung von Menschen und Prozessen

Abgrenzung: Red Teaming



Abgrenzung: Red Teaming

- Festlegung von konkretem Ziel (z.B. Übernahme des *Domain Controllers*)
- Ähnliche Methoden, Tools, Strategien…
- Ergänzt durch Social Engineering
- Längerer Zeitraum der Durchführung
- Überprüfung von Menschen und Prozessen

2. Beispiele

Pentest-Beispiele aus der Praxis

Beispiel: Webanwendung

- Öffentlich erreichbar
- Einstiegspunkt für Zugriff auf interne Netze und Systeme
- Häufig Verarbeitung und Speicherung sensibler Daten
- Webserver ≠ Webanwendung

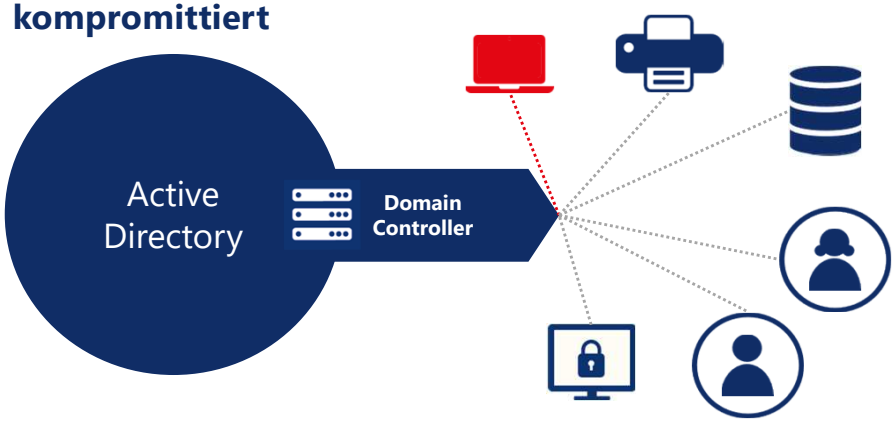
Beispiel: Internes Netzwerk – Angreifer im Netzwerk

- Scope: Intern erreichbare Systeme (nicht authentifiziert)
- Überprüfung von Firewalls und Netzgrenzen
- Identifizierung von Schwachstellen und Sicherheitslücken
- Ausnutzung von Schwachstellen und Rechteausweitung
- Beliebt als Überblick für Ist-Zustand

Beispiel: Internes Netzwerk – Client kompromittiert

- Scope: Windows-Client (authentifiziert)
- Eingebunden in Domäne über Verzeichnisdienst (Active Directory)
- Hohe Komplexität durch viele Objekte (Benutzer, Services, Gruppen)
- Oft (unsichere) Legacy-Protokolle aus Kompatibilitätsgründen
- Domain Controller liefert viele nützliche Infos für Angreifenden
- Angriffsziel: Lokale Rechteausweitung und Lateral Movement

Beispiel: Internes Netzwerk – Client kompromittiert



Beispiel: Internes Netzwerk – Client kompromittiert

- Scope: Windows-Client (authentifiziert)
- Eingebunden in Domäne über Verzeichnisdienst (Active Directory)
- Hohe Komplexität durch viele Objekte (Benutzer, Services, Gruppen)
- Oft (unsichere) Legacy-Protokolle aus Kompatibilitätsgründen
- Domain Controller liefert viele nützliche Infos für Angreifenden
- Angriffsziel: Lokale Rechteausweitung und Lateral Movement

Beispiel: Smartphone-Apps

- Verschiedene Architekturen der Betriebssysteme (iOS & Android)
- Apps werden voneinander isoliert ausgeführt (Sandboxing)
- Interprozesskommunikation stark eingeschränkt
- Sensible Funktionen erfordern Zustimmung
- Zusätzliche Sicherheitsmaßnahmen in Apps (z.B. Root-/Jailbreak-Detection, SSL-Pinning)

Beispiel: Smartphone-Apps

- Verschiedene Architekturen der Betriebssysteme (iOS & Android)
- Apps werden voneinander isoliert ausgeführt (Sandboxing)
- Interprozesskommunikation stark eingeschränkt
- Sensible Funktionen erfordern Zustimmung
- Zusätzliche Sicherheitsmaßnahmen in Apps (z.B. Root-/Jailbreak-Detection, SSL-Pinning)

Beispiel: Smartphone-Apps

- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Pentests von Apps geht schnell Richtung Reverse-Engineering
- App gehärtet oder ungehärtet untersuchen?
- Zielsetzung entscheidend (z.B. Datenschutz, hoher Schutzbedarf)

Beispiel: Smartphone-Apps

- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Pentesting geht schnell Richtung Reverse-Engineering
- App gehärtet oder ungehärtet untersuchen?
- Zielsetzung entscheidend (z.B. Datenschutz, hoher Schutzbedarf)

3. Unklarheiten & Missverständnisse

Metriken und Risikomodelle

- Common Vulnerability Scoring System (CVSS)
- OWASP Risk Rating Methodology
- Eigene Modelle
- Risiko einer Schwachstelle oft kontextabhängig

Metriken und Risikomodelle

- Common Vulnerability Scoring System (CVSS)
- OWASP Risk Rating Methodology
- Eigene Modelle
- Risiko einer Schwachstelle oft kontextabhängig

Sicherheit ist ein Prozess (der nie endet)

- „Sind wir jetzt sicher?“
- „Wir möchten wissen, ob wir sicher sind.“
- Pentests **kein Ersatz** für weitere Sicherheitsmaßnahmen
- **Momentaufnahme** aus Perspektive eines Angreifenden
- Auf den Busch klopfen und gucken was rausfällt

Für den Weg nach Hause…

Komplexität reduzieren

Abhängigkeiten vermeiden

Updaten

Fragen?

Seminare
Webinare
eLearning
Datenschutz und
Informationssicherheit
dsn
Aka
demie
Vielen Dank
für Ihre
Aufmerksamkeit!
Konsul-Smidt-Straße 88 • 28217 Bremen
T +49 (0) 421 69 66 32-298
Mail: akademie@dsn-group.de
www.dsn-group.de