Mit offenen Karten

White Box Application Pentests

it-sa 2022 , 26. Oktober 2022, Jan-Tilo Kirchhoff

Darf ich mich vorstellen?

Jan-Tilo Kirchhoff

- Geschäftsführer Compass Security Deutschland GmbH
- verheiratet, zwei erwachsene Kinder
- Werdegang: Von der TK-Security zur IT-Security
- Kompetenzen
  - Netzwerk Sicherheitsprüfungen
  - ICT- Security (VoIP, PSTN, GSM …)
  - IT-Forensik

Hobbys

- Meine Familie
- Musik (Trompete und Chor)
- Electronic Jazz, Jazz Funk
- Laufsport
- ICT-Security

CISSP® Certified Information Systems Security Professional

OFFENSIVE security [OSCP]®

Red Team Operator

Awarded to Jan-Tilo Kirchhoff

Compass Crew

Was macht Compass?

seit 1999

Penetration Tests

Als Angreifer untersuchen wir Geräte, Netze, Dienste und Anwendungen auf Schwachstellen. Mittels Social Engineering und Red Teaming testen wir das Verhalten der gesamten Organisation.

Digital Forensics

Unsere Forensik-Experten helfen bei der Koordination von Vorfällen und Sofortmassnahmen sowie bei der gerichtsfesten Bearbeitung von Daten. Zudem bieten wir eine unkomplizierte und schnelle Ursachenforschung.

Security Reviews

Erfahrene IT Analysten unterstützen Sie mit Zweitmeinungen zu Security-Konzepten und prüfen nach Wunsch den Aufbau, die Konfiguration und den Quellcode Ihrer Lösung.

Security Trainings

Profitieren auch Sie vom Wissen unserer Analysten zu Penetration Testing, Netzwerkanalyse, sichere Apps und Anwendungen, Digitale Forensik und trainieren Sie in einem eigens dafür erstellten Labor.

Wir sind “nette” Hacker

Bild von Free-Photos auf Pixabay

Tiger Teams

Definitionen (1)

Penetrationstest / Penetrationtest / Pentest
- Eindringversuch

Vulnerability Assessment
- (Umfassende) Suche nach Angriffpunkten

Security Assessment
- (Ganzheitliche) Bewertung der Sicherheit

Red Team
- Angriffssimulation
- (ursprünglich Querdenker/2.Meinung)

Weitere Arten von Sicherheitsprüfungen
- Vulnerability Scans (automatisierte Prüfungen)
- Security Audit (ISO 27000, PCI)

Definitionen (2)

Risiko = Schwachstelle x Bedrohung x Kosten

Schwachstelle (Vulnerability)

- Meist Konfigurations- oder Softwarefehler, die einen möglichen Angriffspunkt darstellen.

Bedrohung (Threat)

- Hier geht es um die tatsächliche bzw. anzunehmende Gefährdung. Wie wahrscheinlich ist es das eine Schwachstelle genutzt wird?

Risiko (Risk)

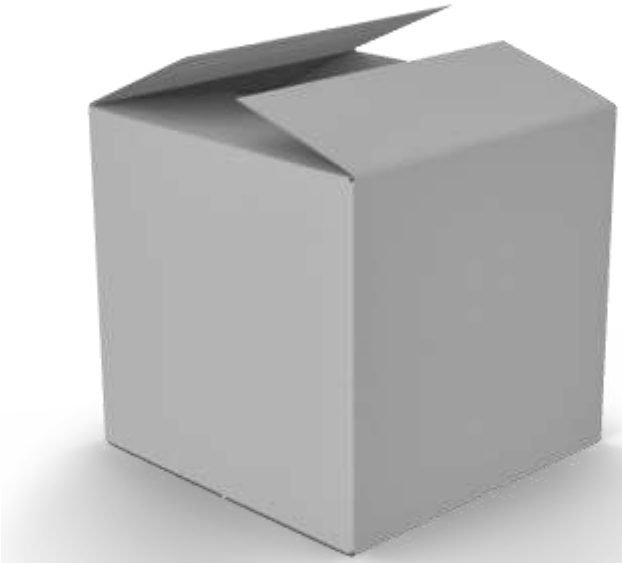
- Die wirtschaftliche Bewertung der Sicherheit

Defintions (3)

Black, White and Gray Box Testing

Ohne Vorwissen

Volle Transparenz



Teilwissen

Whitebox Pentest

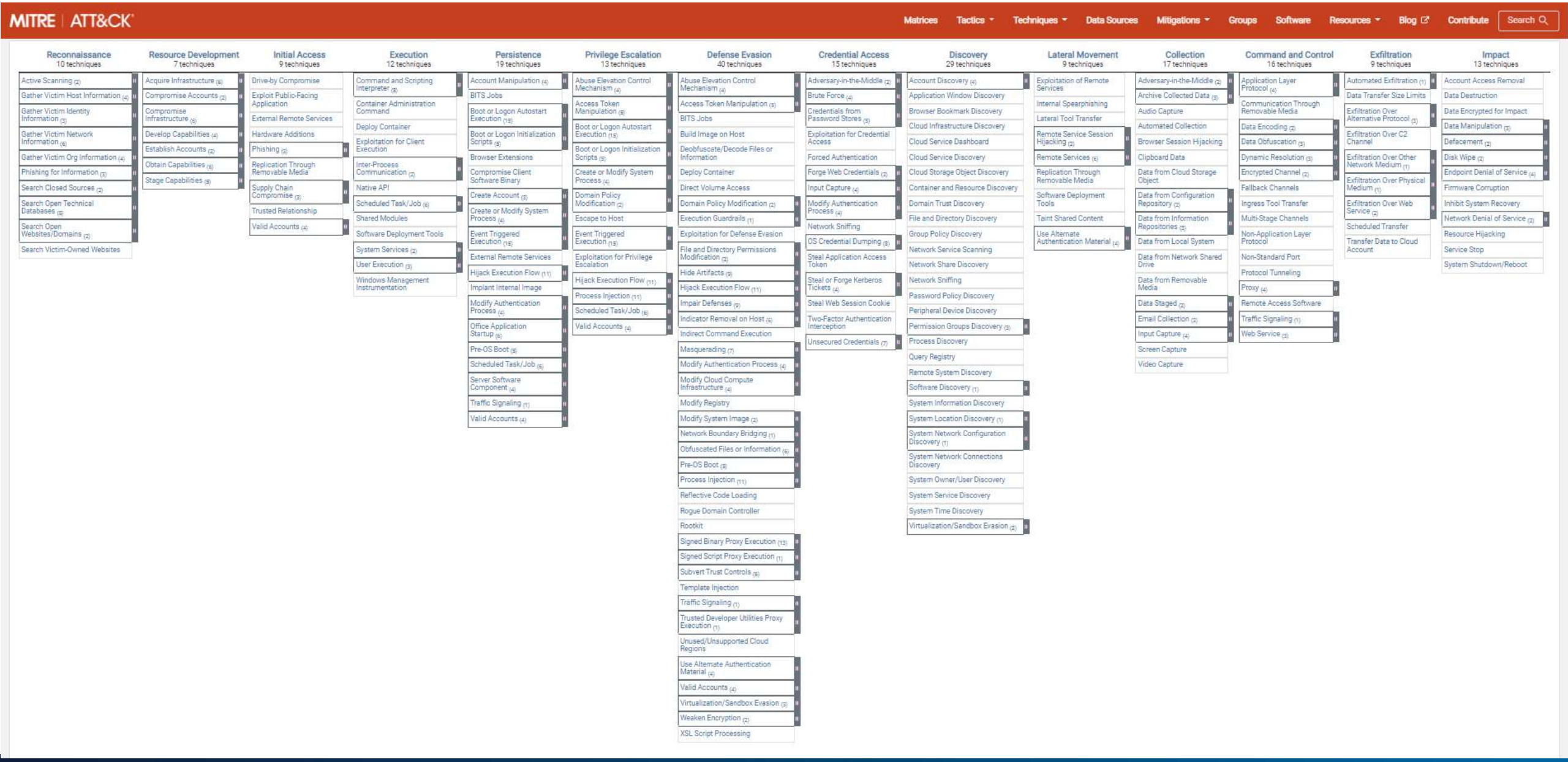
Aus Sicht der Tester

- Bessere Testabdeckung
- Höhere Testtiefe
- Geringerer Zeitaufwand
- Realistischer Ergebnisse

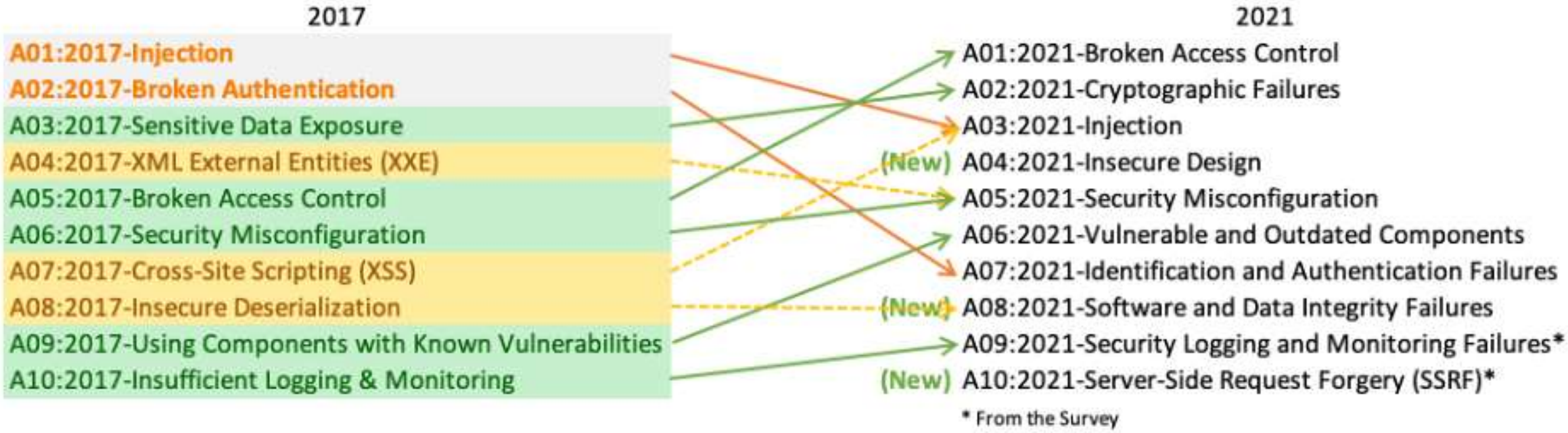
Aus Sicht der Entwickler

- Weniger False Positives
- Präzisere Informationen
- Kürzere Bearbeitungszeiten

Mitre ATT&CK Matrix



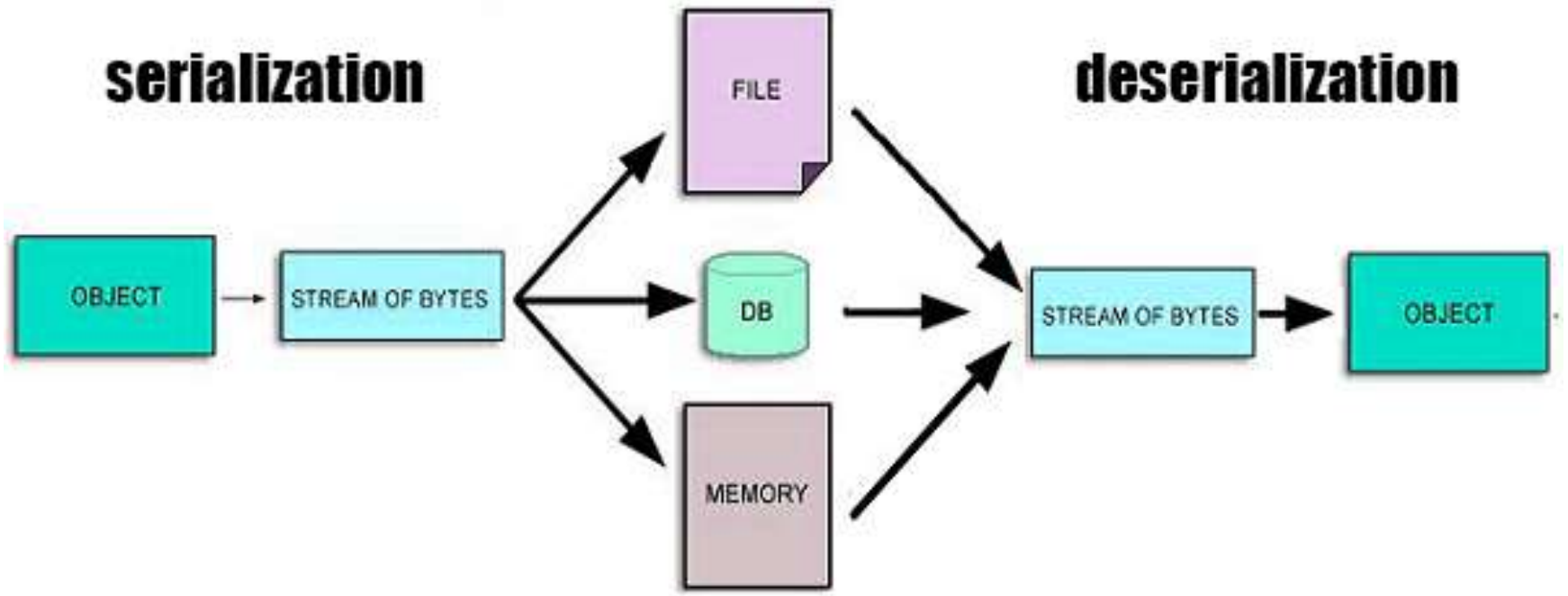
OWASP Top 10 – 2021



A8 Insecure Desirialization (OWASP Top 10 – 2017)

New: “A8 Software and Data Integrity Failures” (OWASP Top 10 -2021)

- Easy to miss and hard to exploit without prior knowledge



Vielen Dank für Ihre Aufmerksamkeit!

Besuchen Sie uns an unserem Messestand

Halle 7 Stand Nr. 7-449

Compass Security Deutschland GmbH
Tauentzienstraße 18
10789 Berlin

team.csde@compass-security.com

Bildnachweis

Aufstellung der Bildquellen, soweit diese nicht von Compass zur Verwendung lizensiert oder selbst angefertigt wurden:

https://upload.wikimedia.org/wikipedia/commons/a/a4/Deutsche_Spielkarten_mit_fr%C3%A4nkischem_Bild.jpg

https://c1.staticflickr.com/5/4081/4809326028_ff2ced002e_b.jpg

https://pixabay.com/de/photos/tiger-raubtier-fell-sch%C3%B6n-4697690/

https://commons.wikimedia.org/wiki/File:Deal_Castle_Aerial_View.jpg

https://www.publicdomainpictures.net/de/view-image.php?image=101786&picture=elefant

https://www.pexels.com/de-de/foto/tier-auge-insekt-schwarzer-hintergrund-9927833/

https://owasp.org/Top10/assets/mapping.png

https://upload.wikimedia.org/wikipedia/commons/f/f4/Serialization.jpg

https://commons.wikimedia.org/wiki/File:S%C3%A1rospatak_-_Castle.jpg

https://upload.wikimedia.org/wikipedia/commons/9/9c/The_Turkish_Siege_of_Vienna.JPG

https://de.wikipedia.org/wiki/30,5-cm-Belagerungsm%C3%B6rser#/media/File:Austro-_hungarian_305_mm_Howitzer.jpg