Mythos Pentest

Offensive Sicherheitsmaßnahmen im Überblick

>> whoami

Moritz Samrock (32)
CBDO und Gesellschafter

- Business Development, OSINT
- M.Eng. Elektrotechnik & Technische Informatik @ UniBw
- MBA Start-Up Development @ H-BRS

- **Mitgründung von Laokoon 2.0**
mit Ex-Bw Hackern Andreas Krüger und Björn Trappe

Email

moritz.samrock@laokoon-security.com

>> whois laokoon-security.com

Laokoon Security GmbH, Bonn-Hardtberg

Gründung 2016
inhabergeführt
+20 Px

Offensive IT-Sicherheitsdienstleistungen

- Red Teaming, inkl. physischer Anteile
- Penetrationstest (OT, Web, Cloud, Container, ...)
- DDoS- und Sensoriktests
- Training

Kunden:
(insbesondere)

- Energieversorger
- Banken & Versicherungen
- Sicherheitsbehörden

https://laokoon-security.com

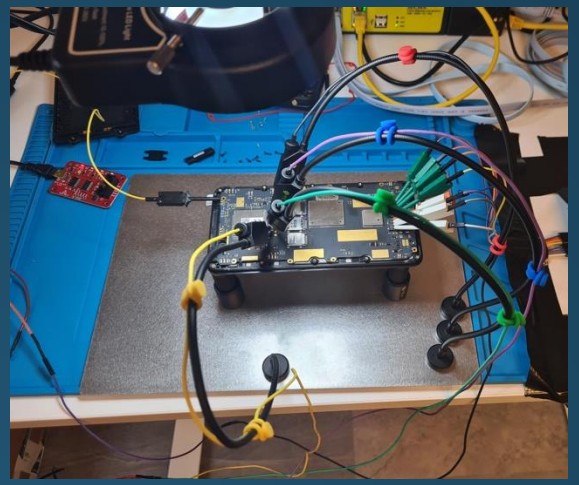
>> whois laokoon-security.com

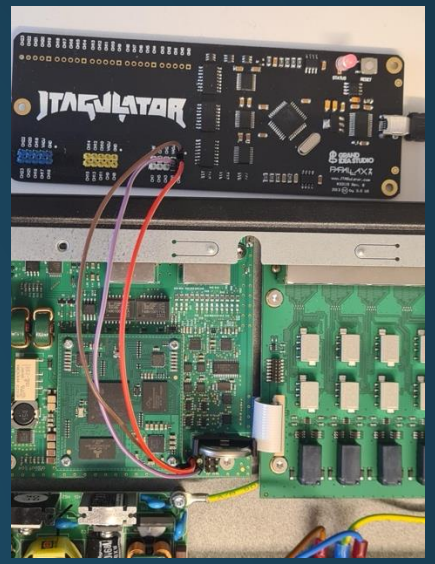
Laokoon SecurITy

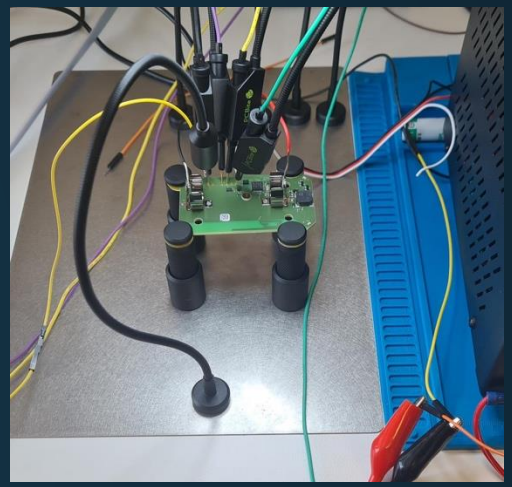
Standort in Bonn

- Sichere on-prem Arbeitsplätze
- Zwei vollausgestatte Labore für Hardwareuntersuchungen
- Dedizierte Infrastruktur für Sicherheitstests

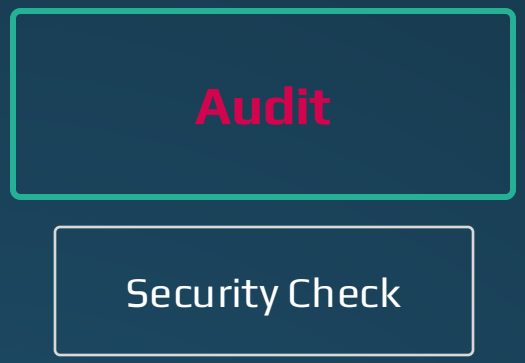
Ausstattung für mobilen Einsatz vor Ort / beim Kunden

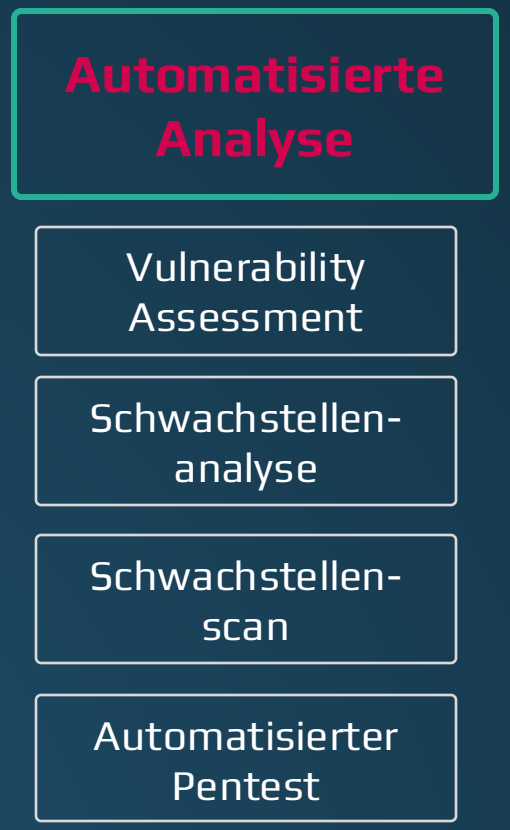


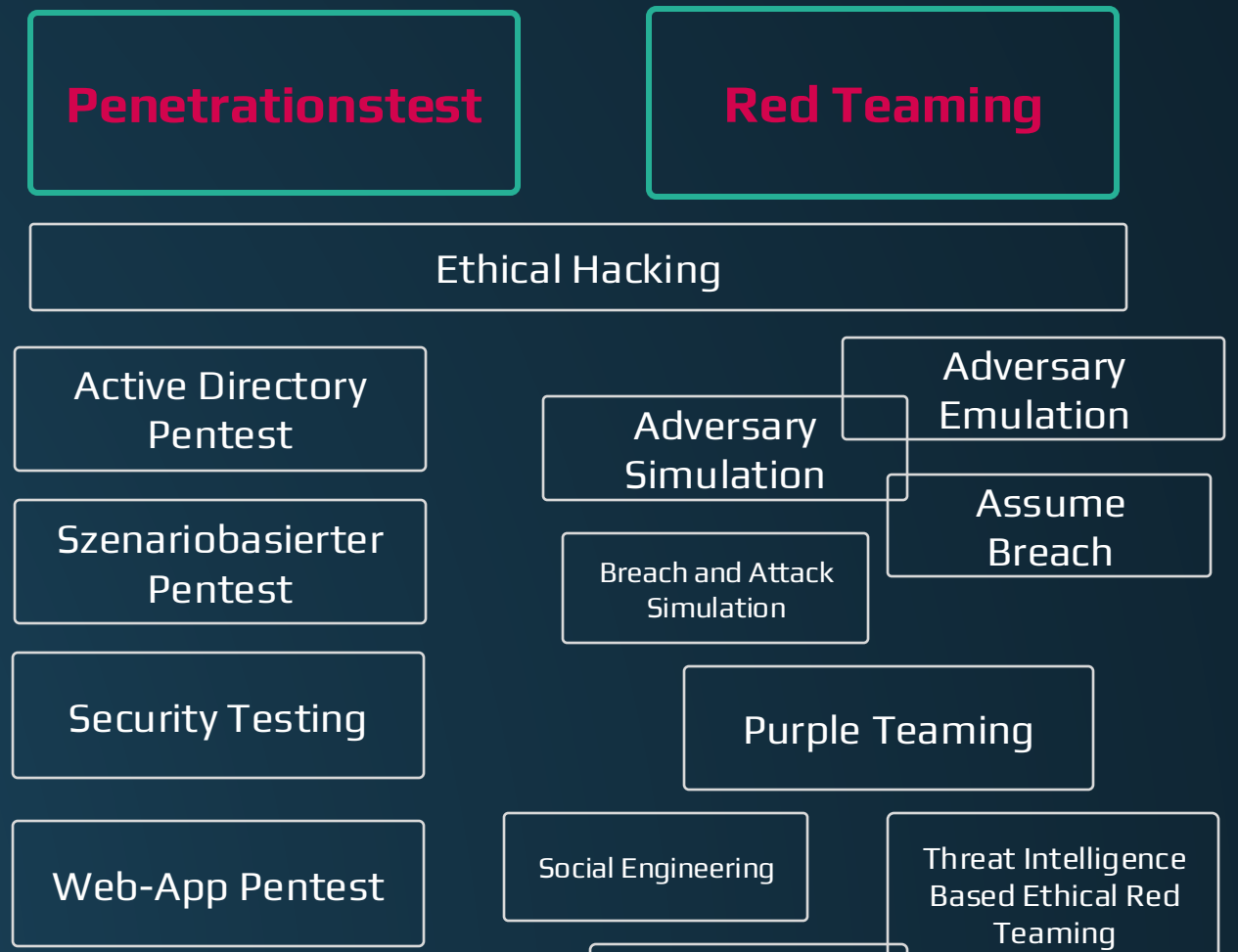





Schwachstellen-scan
Threat-led Penetration Test
Security Review
Purple Teaming
Adversary Simulation
?
Red Teaming
?
Breach & Attack Simulation
Automatisierter Pentest
?
Penetrationstest
Schwachstellen-analyse
Security Testing
Code-Review
?
?
Vulnerability Assessment
?
Web-App Pentest
Threat Intelligence Based Ethical Red Teaming
Sicherheitsaudit
Ethical Hacking
Szenariobasierter Pentest
Adversary Emulation
Security Check
Active Directory Pentest
Assume Breach


Audit
Security Check
Code-Review
Sicherheitsaudit
Security Review


Automatisierte Analyse
Vulnerability Assessment
Schwachstellen-analyse
Schwachstellen-scan
Automatisierter Pentest


Penetrationstest
Ethical Hacking
Active Directory Pentest
Szenariobasierter Pentest
Security Testing
Web-App Pentest

Red Teaming
Adversary Emulation
Adversary Simulation
Assume Breach
Breach and Attack Simulation
Purple Teaming
Social Engineering
Threat Intelligence Based Ethical Red Teaming
Threat-led Penetration Test

Ziele & Art der Durchführung

	Audit	Automatisierte Analyse	Penetrationstest	Red Teaming
Ziele	Nicht-intrusive Übersichtsgewinnung über Sicherheitsniveau	Systeme identifizieren, die bekannte Schwachstellen haben	Identifikation möglichst aller bekannter und unbekannter technischen Schwachstellen in definierten Systemen oder Systemverbünden	Analyse der Angriffserkennungs- und verhinderungssysteme sowie der Reaktionsfähigkeit der Verteidiger (Blue Team)
Art d. Durchführung	Interviews mit Verantwortlichen Checklisten Dokumentations-analyse	Automatisiertes Scanning mit Host-Detektion und Überprüfung mittels PoC-Skripten	Teilautomatisierte und manuelle Überprüfung der zu prüfenden Systeme	Manuelle Angriffs-durchführung

Auftraggeber & Eingeweihter Personenkreis

	Audit	Automatisierte Analyse	Penetrationstest	Red Teaming
Auftraggeber	CISO, Informationssicherheitsbeauftragter, Geschäftsführer, IT-Leiter, Kunde	IT-Leiter, Infrastruktur- oder Produkt-verantwortlicher	IT-Leiter, Infrastruktur- oder Produkt-verantwortlicher, Kunde	CISO, IT-Sicherheitsmanager, SOC-Leiter
Eingeweihte	Keine Einschränkung, Betroffene Personen (Interviewpartner)	Auftraggeber, Administratoren, SOC-Leiter und Mitarbeiter, ...	Auftraggeber, System-verantwortliche, ...	Auftraggeber, “White Team/Cell“

Testumgebung, Vorgehen & Folgemaßnahmen

	Audit	Automatisierte Analyse	Penetrationstest	Red Teaming
Testumgebung	Produktivsysteme	Produktivsystem	Produktiv- oder Testsystem (bevorzugt)	Produktivsystem
Maßnahmen	Organisatorische Maßnahmen, tiefergehende Analysen	Konfigurations-anpassungen und Updates	Konfigurations-anpassungen, Komponenten-updates und Patchentwicklung	Anpassung Angriffserkennung (XDR, SOC, ..), Blue Team Schulungen, Organisatorische Maßnahmen
Vorgehen	Offenes Vorgehen	Offenes Vorgehen	Verdecktes oder offenes Vorgehen (empfohlen)	Verdecktes Vorgehen

Dauer, Kosten & Anforderungen

	Audit	Automatisierte Analyse	Penetrationstest	Red Teaming
Dauer	Tage bis Wochen	Stunden bis Tage	Tage bis Wochen	Wochen bis Monate
Kosten	Niedrig bis Mittel	Niedrig	Mittel bis erhöht	Mittel bis hoch
Anforderungen	Fachliche Expertise, Kommunikations-fähigkeiten	Administration, Systemverständnis	Tiefe fachliche Expertise, Kommunikations-fähigkeit	Tiefe fachliche Expertise, Verdecktes Vorgehen, Kommunikations-fähigkeit

Was kann alles gepentestet werden?

Laokoon SecurITy

Netzwerke

Netzwerke und Netzwerksegmente, intern & extern, "Der Klassiker"

Anwendungen

Anwendungen aller Art (Web, Desktop, Smartphone, ...), (Black | Gray | White)-Box

Verzeichnisdienste (AD)

Fehlkonfigurationen, Missbrauch von Rechten, Privilegemanagement, "Überbleibsel"

OT- und IoT-Geräte

Hardwarenah, K3s, Linux

Cloud und IaaS

Fehlkonfigurationen, Rechtemanagement, Sichtbarkeiten

Container und Cluster

Fehlkonfigurationen, Rechtemanagement, Sichtbarkeiten

Laokoon SecurITy

Black-Box-Test

Tester haben keine Informationen

White-Box-Test

Tester haben uneingeschränkte Informationen (Source-Code & Logs & Nutzerrechte)

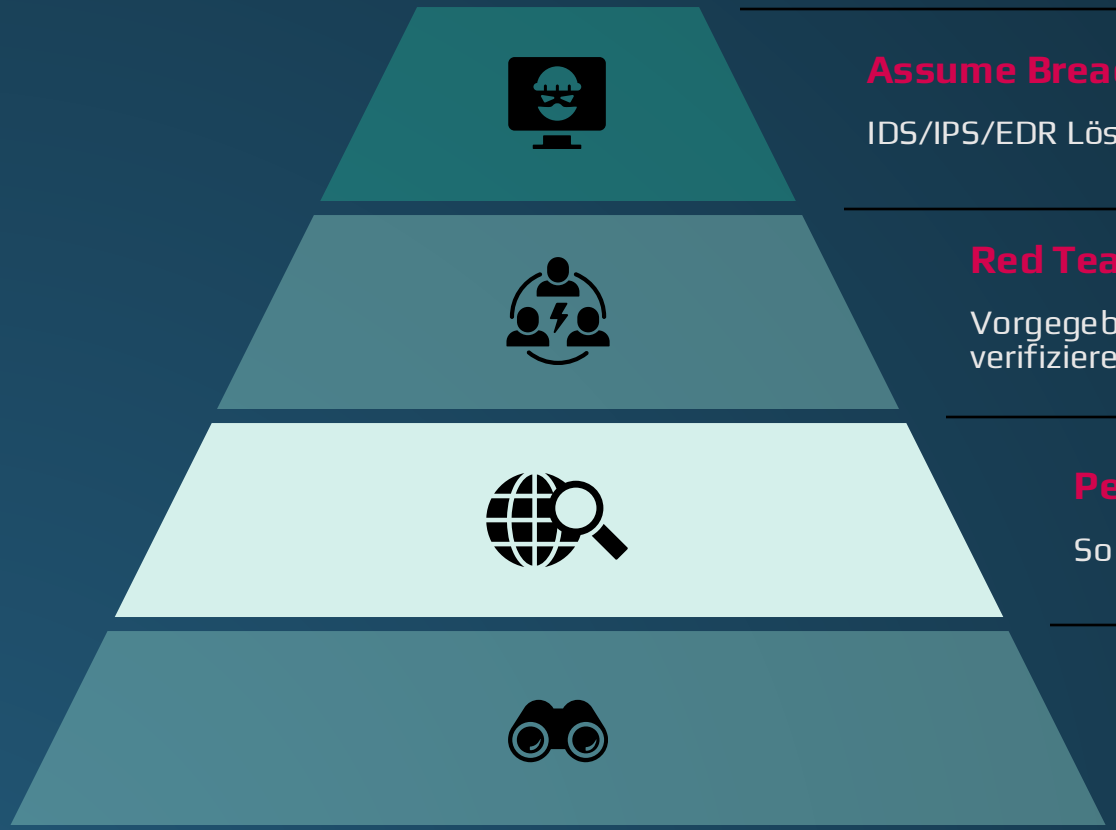
Gray-Box-Test

Tester haben teilweise Informationen (Source-Code | Logs | Nutzerrechte)

Offensive Security Stack

Penetration Test – oder doch was anderes?

"It isn't normal to know what we want. It is a rare and difficult psychological achievement." Abraham Maslow



Assume Breach/Blue Team Training

IDS/IPS/EDR Lösungen auf Effektivität prüfen, Verteidiger trainieren

Red Teaming und Attack Simulation

Vorgegebenes Ziel erreichen, Reaktionsvermögen prüfen, Gefahrenpotenziale verifizieren

20 %

Penetrationstest

So viele wie möglich Schwachstellen in Entität finden.

(automatisierter) Schwachstellenscan

Bekannte Schwachstellen und Konfigurationsfehler aufspüren, Assets überprüfen und Schatten-IT finden

80 %

Mythos Pentester

Eigenschaften eines Hackers im Überblick

Warum Pentester werden?

Fragestellungen:

- Warum möchtest Du Penetrationstester/ Hacker werden?
- Warum nicht:
  - Cyber Security Engineer
  - SOC-Analyst
  - Incident Responder
  - IT-Forensiker
  - IT-/Info-Sicherheitsmanager
  - ...

Eigenschaften eines Penetrationstesters

- Technische Expertise
  - Skripting in Python
  - Systemverständnis (Web-Applikationen, Unternehmensnetzwerke, ggf. OT, ..)
  - Absolut feste Basis
    - ISO/OSI-Modell
    - Fortgeschritten in Linux und Microsoft Betriebssystemen
    - Active Directory
    - Web-Protokolle
    - Uvm.
- Kommunikationsfähigkeit
  - in Wort und Schrift
- Beharrlichkeit
- Frustrationstoleranz

Was ein (Senior-)Pentester macht

- Kunden v… die Richtige f…
- Projektfü… …r führen)
- Pentestin…
  - Im Scop…
- **Reportin…**
  - Dokume…
  - Was sin… …enutzt werden…

Nobody cares,
was für ein krasser Hacker du bist,
wenn Du deinem Kunden nicht auf verständliche Arte und Weise darstellen kannst,
was das Problem, das Risiko und die Lösung ist.

Let‘s connect!