more security. usd

usd HeroLab

PENTEST

LEISTUNGSBESCHREIBUNG

Stand: September 2019

KÖNNEN HACKER IN IHRE SYSTEME EINDRINGEN?

UNSERE PENTESTS LIEFERN ANTWORTEN

usd Pentests bieten Ihnen die Möglichkeit, Ihre Infrastruktur individuell von einem unserer Sicherheitsexperten des usd HeroLabs überprüfen zu lassen. Der durchführende Sicherheitsexperte übernimmt legal die Rolle eines Hackers und versucht gezielt, individuell und erfinderisch, in Ihre Systeme einzudringen. Diese Simulation eines realen Hackerangriffs liefert qualitativ hochwertige Ergebnisse, die wir gemeinsam mit konkreten Verbesserungsvorschlägen für Sie in Berichtsform übergeben.

MÖGLICHE PRÜFBEREICHE

Sie bestimmen, was geprüft werden soll. Ziel und Umfang des Pentests legen wir individuell mit Ihnen fest. Folgende Komponenten können dabei einzeln oder kombiniert Bestandteil sein. Sollte Ihnen etwas fehlen, sprechen Sie uns gerne an.

- Webapplikationen
- IT-Systeme (externe & interne Perspektive)
- Mobile Applikationen
- Fat Client
- Wireless LAN

UNSER VORGEHENSMODELL

Internationale Standards und langjährige Erfahrungen bilden die Basis unseres Vorgehensmodells, das Effizienz und Qualität garantiert. Vorgaben des NIST SP800-115, Anforderungen des PCI DSS sowie Handlungsempfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI), des Open Web Application Security Project (OWASP) und Open Source Security Testing Methodology Manual (OSSTMM) werden berücksichtigt. Das Pentest Service Management begleitet Sie während des gesamten Projektverlaufes.

KICK-OFF-VORBEREITUNG

Unser Pentest Service Management unterstützt Sie bei der Informationsbeschaffung der für den Kick-off relevanten Dokumente und Informationen.

KICK-OFF-MEETING

Im Kick-off-Meeting mit den technischen und organisatorischen Verantwortlichen Ihres Hauses erfolgt die Vorbereitung des Pentest. Hierbei wird die zu prüfende IT-Infrastruktur spezifiziert, notwendige Benutzerkonten und Zugriffswege abgestimmt, Ansprechpartner und Eskalationswege definiert sowie der Testablauf im Detail gemeinsam besprochen.

INFORMATION GATHERING

In dieser Phase werden Informationen über die im Kick-off spezifizierten Ziele gesammelt. Neben einem Portscan wird auch ein Schwachstellenscan durchgeführt. Mögliche Schwachstellen werden noch nicht ausgenutzt. Diese Phase dient unseren Sicherheitsexperten als Vorbereitung für die aktiven Eindringversuche der Exploitation Phase.

MANUAL RESEARCH

Die im Verlauf der vorherigen Phasen gefundenen Informationen werden auf ihre Bedeutsamkeit untersucht. Vorliegende Daten werden durch unsere Sicherheitsexperten verglichen und bezüglich ihrer Konsistenz geprüft. So werden potentielle Schwachstellen identifiziert.

EXPLOITATION

In dieser Phase wird versucht, die identifizierten Schwachstellen auszunutzen, um aktiv Zugriff auf die Zielsysteme und gespeicherten Daten zu erlangen. Dabei werden von unserem Sicherheitsteam, abhängig vom jeweiligen Dienst oder der technischen Umgebung, neue Exploits geschrieben oder bestehende verwendet. Kritische Schwachstellen werden nur nach Rücksprache ausgenutzt. Potentielle Schwachstellen können sich hier als falsch-positiv herausstellen. Nur verifizierte Schwachstellen werden in den abschließenden Bericht aufgenommen und entsprechend ihrer Kritikalität eingestuft.

REPORT

Sie erhalten einen umfassenden Bericht bestehend aus einer Executive Summary und einem Technical Report in Deutsch oder Englisch. Darin wird die Kritikalität von Findings und Eintrittsrisiken bewertet sowie Maßnahmenempfehlungen gegeben.

REMEDIATION

In dieser Phase erfolgt die Beseitigung der identifizierten Abweichungen bzw. Schwachstellen durch Ihr Haus. Bei Bedarf werden Sie hierbei fachlich durch unsere erfahrenen Berater unterstützt. Optional stellt Ihnen unser Pentest Service Management ein Fortschritts-Tracking inklusive Übersicht gefundener Schwachstellen und Statusabfrage zur Verfügung.

OPTIONALE NACHPRÜFUNG

Sie haben die Möglichkeit, nach Durchführung der Remediation eine Nachprüfung durch uns durchführen zu lassen. Hierbei überprüfen wir die Wirksamkeit Ihrer Maßnahmen.

ZERTIFIKAT

Wenn Ihre Pentestergebnisse die Anforderungen des PCI DSS erfüllen, bestätigen wir Ihnen dies gerne in einem persönlichen Zertifikat. So können Sie auch Dritten Ihren Anspruch an Sicherheit demonstrieren.

SIE HABEN EINE GRÖSSERE UMGEBUNG?

Unser Pentest Service Management unterstützt Sie bei der Vorbereitung und Durchführung Ihrer Pentests – plattformgestützt durch usd Security Connect. Optionale Remediation-Leistungen können hier abgebildet und in Ihre Prozesse integriert werden. Die Grundlage für ein effizientes Prozess- und Schwachstellenmanagement ist die Integration von Security Connect in Ihr Unternehmen. Ihre Assets, Ihre Ansprechpartner und Ihr Pentteststatus werden hier abgebildet. Gerne unterstützen wir Sie beim Rollout und schulen auf Wunsch Ihre Mitarbeiterinnen und Mitarbeiter.

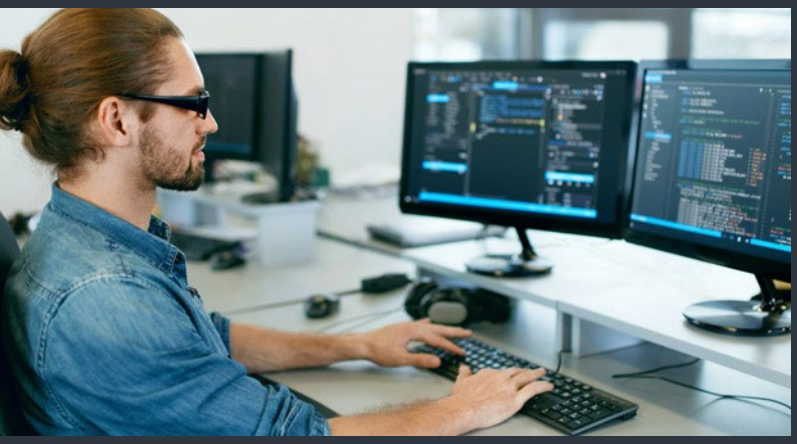
TIPPS ZUM PENTESTINTERVALL

Stetig werden neue Schwachstellen, beispielsweise durch Hacker-Angriffe, entdeckt. Veränderungen der IT-Umgebung, z. B. durch Softwareaktualisierungen, können zu neuen Sicherheitslücken führen.

Daher sollten Pentests regelmäßig im Zeitraum von 6 Monaten wiederholt werden und fest in den Sicherheitsprozess integriert werden. Gerne unterstützen wir Sie hierbei!

WIE WIR ARBEITEN

UNSER TEAM



Unser Team aus rund 80 hochqualifizierten Security Analysten verfügt über zahlreiche Sicherheitszertifizierungen und umfangreiche Erfahrung aus internationalen Projekten. Jedes Teammitglied bildet sich kontinuierlich weiter und spezialisiert sich auf ein Fachgebiet; so kombinieren wir Expertenwissen aus verschiedenen Teilbereichen der IT Sicherheit. Gemeinsam mit Kolleginnen und Kollegen unseres Pentest Service Managements garantieren wir Ihnen Managed Security Services aus einer Hand – integriert in Ihre Organisation.

EFFIZIENZ & QUALITÄT

Der hohe Automatisierungsgrad unserer Prozesse sowie das exzellente Know-how unserer Security Analysten sind der Qualitätsgarant unserer Arbeit. Wir verwenden eigenentwickelte, qualitätsgesicherte Tools sowie Tools international anerkannter Hersteller. Dies ermöglicht es uns, Prüfungen noch effizienter und umfassender durchzuführen und lässt Zeit für gezielte manuelle Analysen.

UNSERE ZERTIFIZIERUNGEN

Unsere Sicherheitsexperten sind alle nach dem „usd HeroLab Certified Professional“ (UCP) und nach international anerkannten Standards zertifiziert:

- OSCP Offensive Security Certified Specialist
- OSCE Offensive Security Certified Expert
- SANS FOR408: Windows Forensic Analysis
- SANS SEC504: Hacker Tools, Techniques
- EXPLOITS AND INCIDENT HANDLING
- SANS SEC575: Mobile Device Security
- CEH Certified Ethical Hacker
- CISA Certified Information Systems Auditor
- CISM Certified Information Security Manager
- ITIL IT Infrastructure Library

UNSERE TOOLS & PLATTFORMEN

Wir stellen die höchsten Ansprüche an die Qualität unserer Arbeit. Um Sicherheitsanalysen immer mit gleichbleibender Effizienz und Qualität durchzuführen, unterliegen unsere eigenen Tools strengen Qualitätsmanagement- und Optimierungsprozessen. Die Ergebnisse unserer Forschung fließen dabei fortlaufend ein.

usd SECURITY CONNECT

Unsere Plattform für gemeinsames Prozess- und Schwachstellenmanagement.

Außerdem ermöglicht die Plattform das Einspielen von Assets, die Zuordnung von Verantwortlichen, ein sicheres Rollen- und Benutzerkonzept, das Buchen von Sicherheitsanalysen, die Erstellung von individuell konfigurierbaren Berichten und Dashboards, das Einsehen identifizierter Schwachstellen und des Remediation-Prozesses sowie ein integriertes Servicemanagement. Gemeinsam agieren. Transparent, sicher und effizient.

usd ICEBREAKER

Analysewerkzeug für alle Teammitglieder.

Der usd Icebreaker verbindet die besten öffentlich vorhandenen und usd intern entwickelten Tools für die Sicherheitsanalyse von Systemen und Anwendungen. Unsere Wissensdatenbank für ein gleichbleibend hohes Qualitätsniveau Ihrer Überprüfungen.

usd ExPeRT

Unterstützt alle Teammitglieder bei der Planung und der Zusammenarbeit während eines Projekts.

Abbildung unserer langjährigen bewährten internen Prozesse für die Durchführung von Pentests und Sicherheitsanalysen. Integrierte Checklisten für eine überprüfbare, einheitliche und qualitativ hochwertige Projektdurchführung.

usd REPORTING TOOL

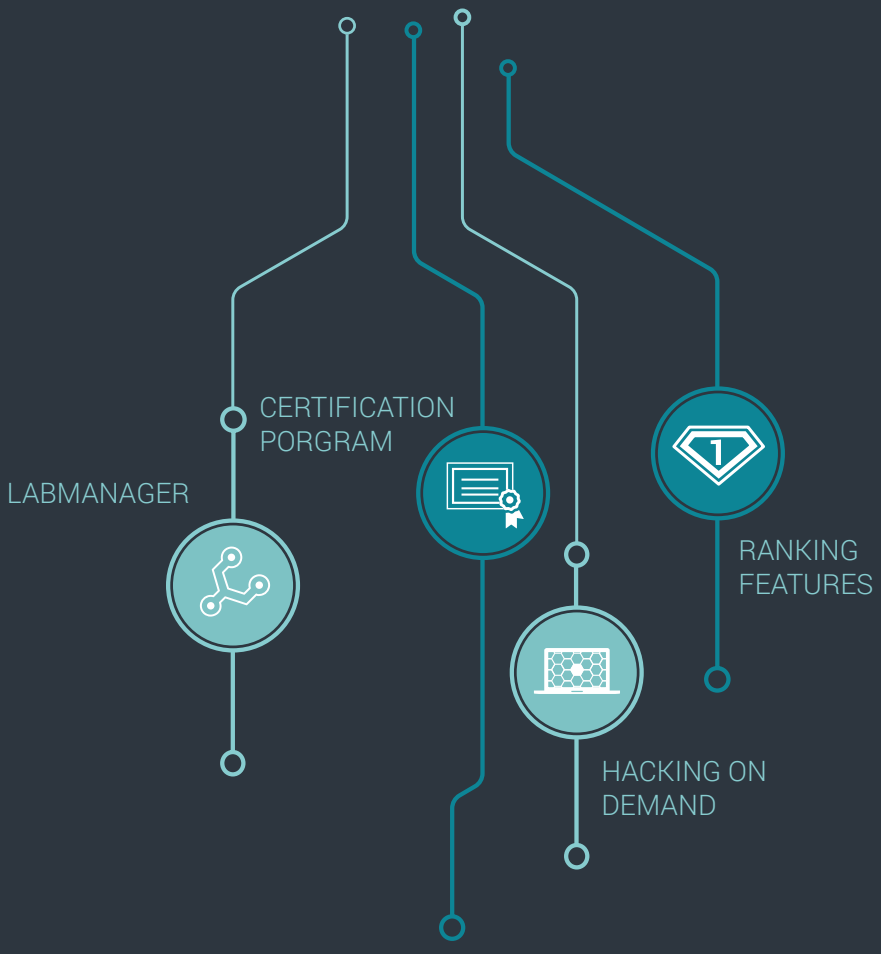
Das Ergebnis unserer Analysen für Sie aufbereitet.

Erhalten Sie einheitlich verfasste Berichte von gleichbleibend hoher Qualität. Identifizierte Schwachstellen werden ausführlich erläutert, die Gefahren und mögliche Auswirkungen beschrieben - inklusive Maßnahmenempfehlungen zur Behebung.

DAS PENTESTLAB

Das Herzstück unserer Technologie-Umgebung.

Mit einer ständig wachsenden Anzahl vorkonfigurierter Serverumgebungen, unterschiedlicher Technologien und Schwachstellen stellt das usd PentestLab unsere Trainings-, Forschungs- und Veranstaltungsumgebung dar.



ÜBER DIE usd AG

WIR SCHÜTZEN UNTERNEHMEN VOR HACKERN UND KRIMINELLEN.

So dynamisch und vielfältig wie die Bedrohung ist unsere Arbeit. Als akkreditierter Auditor beraten und zertifizieren wir Unternehmen nach den Vorgaben der Kreditkartenindustrie weltweit. Die Experten des usd HeroLabs identifizieren Schwachstellen in IT-Systemen und Applikationen. Unsere Security Consultants beraten Unternehmen ganzheitlich in Fragen der Informationssicherheit, des Risikomanagements und der IT-Compliance. Wir tragen Verantwortung, die Cyber Security Transformation Academy (CST Academy) fördert Austausch und Wissenstransfer in der Community. more security ist unsere Mission.

KONTAKTIEREN SIE UNS GERNE.

Im kostenfreien Erstgespräch sprechen wir über Ihre Ziele, Umgebungen und potentielle Risiken. Erst dann erhalten Sie ein passgenaues Angebot.

IHR ANSPRECHPARTNER

Daniel Heyne
usd Sales Representative,
Security Consultant Pentest, OSCP, OSCE

Telefon: +49 6102 8631–190 | Mail: vertrieb@usd.de
PGP oder S/MIME für verschlüsselte Kommunikation