more security. usd

usd HeroLab

PENTEST

SERVICE DESCRIPTION

Status: December 2020

CAN HACKERS PENETRATE YOUR SYSTEMS?

OUR PENTESTS PROVIDE RELIABLE RESULTS

usd pentests offer you the opportunity to have your IT infrastructure individually tested by one of our usd HeroLab security analysts. The security analyst performing the pentest will assume the role of a hacker and try to penetrate your systems legally using a targeted, individual and creative approach. This simulation of a real hacking attack delivers high-quality results, which we present to you in the form of a report which also includes practical suggestions for improvement.

POSSIBLE TESTING AREAS

You decide what needs to be tested. Together, we individually discuss and decide on your pentest targets and scopes. The following components might be used separately or combined with each other. If you need something not included on this list, don't hesitate to contact us.

- IT Systems (external/internal)
- Webapplications
- Mobile Applications
- Cloud
- Fat Clients

OUR APPROACH

International standards and many years of experience are the basis of our approach, guaranteeing efficiency and quality. NIST SP800-115 specifications, PCI DSS requirements and recommendations of the German Federal Office of Information Security (BSI) and the Open Source Security Testing Methodology Manual (OSSTMM) are taken into account. Our Pentest Service Management supports you throughout your entire pentest project.

KICK-OFF PREPERATION

Our Pentest Service Management supports you in the acquisition of information, documents and information relevant for the kick-off.

KICK-OFF-MEETING

The pentest is prepared at a kick-off meeting with the responsible technical and organizational specialists of your company. In this meeting, we specify the IT systems to be tested, coordinate necessary user accounts and access channels, define contact partners and escalation channels and discuss the test procedure in detail.

INFORMATION GATHERING

During this phase, we gather information about the IT systems specified in the kick-off meeting. In addition to a port scan, we also perform a vulnerability scan. In this step, we will not yet exploit vulnerabilities that we've identified. This phase helps to prepare our security analysts for the active penetration attempts to be performed in the exploitation phase.

MANUAL RESEARCH

The information gathered during the previous phase is examined as to its relevance. Our security analysts compare existing data and evaluate it regarding its consistency. In this way, potential vulnerabilities are identified.

EXPLOITATION

In this phase, we attempt to exploit the identified vulnerabilities to actively obtain access to the target systems and to stored data. Depending on the specific service or the technical environment, our security analysts either write new exploits or use existing ones. Potential vulnerabilities might turn out false-positive in this process. Only verified vulnerabilities are included in the final report and classified according to their criticality.

REPORT

You will receive a comprehensive report comprising an Executive Summary and a Technical Report. This report contains an evaluation of the criticality of the findings and their risks of occurrence. It also includes recommendations for corrective action.

REMEDIATION

In this phase, employees of your company eliminate identified deviations and vulnerabilities. If required, you will be supported by our experienced consultants. Optionally, our Pentest Service Management keeps you updated on the progress and provides you an overview of all vulnerabilities found and a status query.

OPTIONAL RE-TESTING

On request, we conduct a re-test after you have completed your remediation to verify its effectiveness.

CERTIFICATE

If the pentest results meet the requirements of PCI DSS, we will gladly issue you with our security certificate. This enables you to demonstrate to third parties that you take security seriously.

YOU HAVE A LARGER ENVIRONMENT?

Our Pentest Service Management will support you in preparing for and conducting your pentests - via our platform usd Security Connect. Optional remediation services can be implemented here and integrated into your processes. The basis for an efficient process and vulnerability management is the integration of the platform into your company. Your assets, primary contacts and the status of your pentests are displayed here. We are happy to support you during the rollout and train your employees if desired.

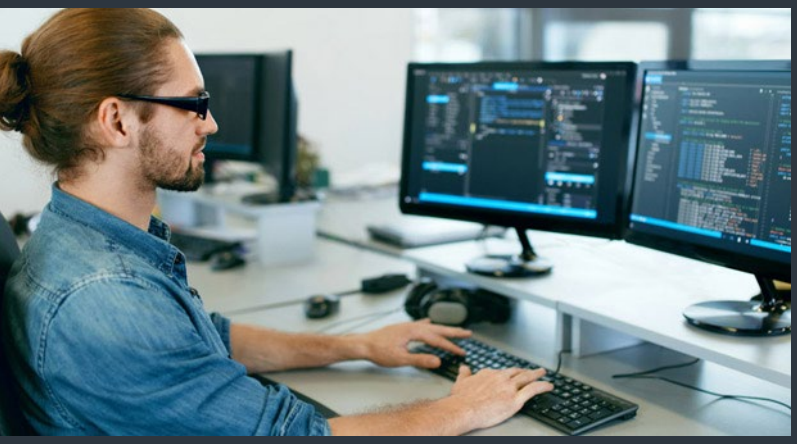
TIPS FOR THE PENTEST INTERVAL

New vulnerabilities are constantly being discovered, e.g., through hacking attempts. Changes to the IT environment, such as software updates, can lead to new security vulnerabilities.

Pentests should therefore be repeated in regular intervals over a period of 6 months and be firmly integrated into your security processes. We are happy to support you in achieving this!

THE WAY WE WORK

OUR TEAM



Our team of approximately 80 highly qualified security analysts are certified according to internationally recorgnized standards and have extensive experience working in international projects. Each team member undergoes contiuous training and specializes in an expert field; this way we combine expertise from different subdisciplines of IT security. Together with our Pentest Service Management Team, we guarantee you managed security services from a single source - integrated into your organization.

EFFICIENCY & QUALITY

The high degree of automation of our processes and the excellent know-how of our around 80 security analysts ensure the quality of our work. We use tools developed and quality assured in-house as well as tools from internationally recognized manufactures. This allows our security analysts to carry out their tests even more efficiently and comprehensively and leaves more time for targeted, manual analyses.

OUR CERTIFICATIONS

All of our security analysts are certified according to “usd HeroLab Certified Professional” (UCP) and internationally recognized standards:

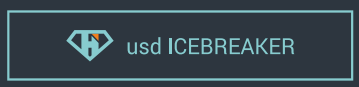
- OSCP Offensive Security Certified Professional
- OSCE Offensive Security Certified Expert
- SANS FOR408: Windows Forensic Analysis
- SANS SEC504: Hacker Tools, Techniques
- EXPLOITS AND INCIDENT HANDLING
- SANS SEC575: Mobile Device Security
- CEH Certified Ethical Hacker
- CISA Certified Information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

OUR TOOLS & PLATFORMS

We place the highest demands on the quality of our work. To ensure that security analyses are always carried out with constant efficiency and quality, our own tools are subject to strict quality management and optimization processes, always taking into account the findings of our research.

Our platform for joint process and vulnerability management.

The platform features importing assets, assigning responsible persons, a secure role and user concept, booking security analyses, creating customizable reports and dashboards, viewing identified vulnerabilities and remediation processes as well as an integrated service management. Acting together. Transparent, secure and efficient.



Analysis tool for all team members.

The usd Iebreaker combines the best publicly available tools and usd in-house developments for security analyses of systems and applications. Our knowledge database for a consistently high quality level of your security analyses.

Project planning and collaboration support for all team members.

Mapping of our long-standing proven internal processes for pentests and security analyses. Integrated checklists for verifiable, consistent and high-quality project implementation.

usd REPORTING TOOL

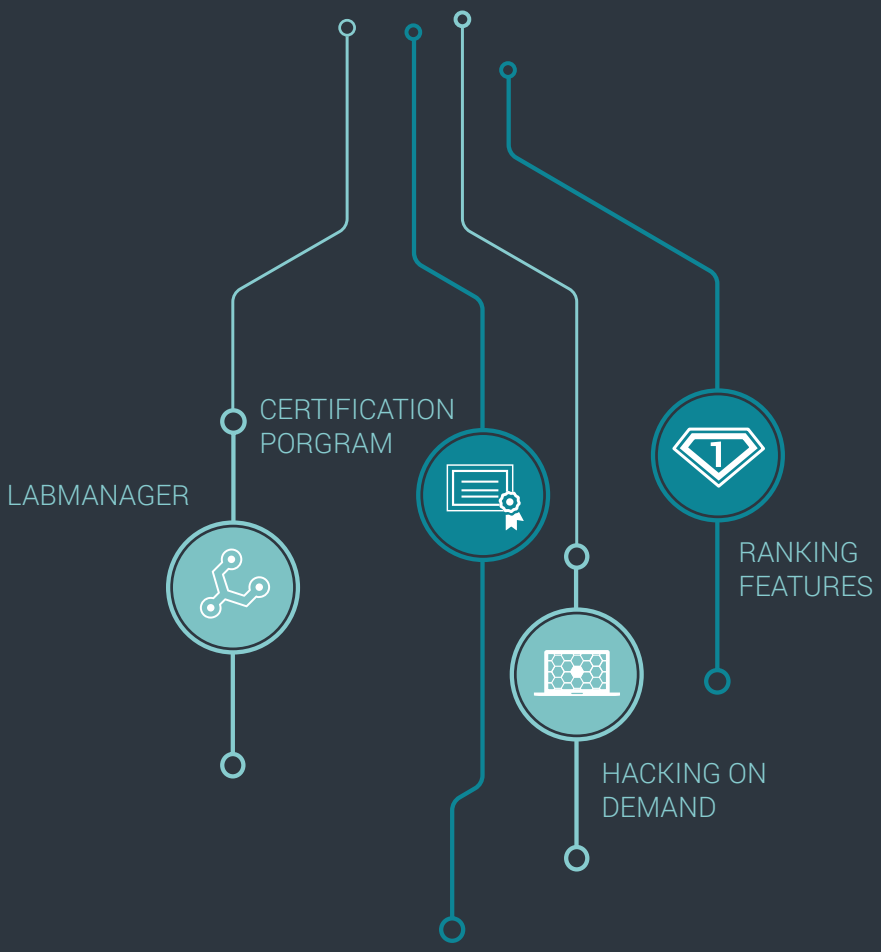
The results of our analyses prepared for you.

Receive consistent high quality reports. Identified vulnerabilities are explained in detail and threats and potential impacts are described. For each vulnerability, you receive recommendations for a fast and verifiable remediation.

THE PENTESTLAB

The heart of our technology environment

With a constantly growing number of preconfigured server environments, different technologies and vulnerablities, the usd PentestLab represents our training, research and event environment.



ABOUT usd AG

WE PROTECT COMPANIES AGAINST HACKERS AND CRIMINALS.

Our work is as dynamic and diverse as the threat itself. As an accredited assessor, we advise and certify companies worldwide according to the specifications of the credit card industry. The experts at usd HeroLabs identify vulnerabilities in IT systems and applications. Our security consultants advise companies holistically on questions of information security, risk management, and IT compliance. The Cyber Security Transformation Academy (CST Academy) promotes exchange and knowledge transfer within the community. more security is our mission.

PLEASE CONTACT US.

In a free initial consultation, we will talk about your goals, environments and potential risks. Only afterwards will you receive an offer that is truly tailored to your needs.

YOUR CONTACT PERSON

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

Phone: +49 6102 8631–190 | Mail: sales@usd.de
PGP oder S/MIME for secure communication.