PENETRATION TESTING (PENTEST)

Delivered by Pentastic Security Limited

Exploiting vulnerabilities within a time constraint.

OVERVIEW

Pentest is widely referred to as ethical hacking. With client consent to a carefully designed project scope and rules of engagement, we model the activities of real-world threats to discover vulnerabilities. Through controlled exploitation in a professional manner, we attempt to determine risk and impact associated with these flaws. Our consultant team recommends appropriate defense solutions to help clients strengthen the security posture.

Clients can use Pentest to assess the effectiveness of their existing suite of security controls more proactively to address and mitigate cybersecurity risk, which may have consequences affecting their operations, financials and reputation.

OPPORTUNITIES

The key value for Pentest is to find out vulnerabilities which cannot be discovered by an automatic scanner. Pentest using manual effort requires skilled and experienced experts. Companies use outsourcing vendor to provide pentest service can tackle both talent shortage and independence issues. Our consultant has quality offensive security accreditations such as OSCP, OSWP, focusing on hands-on skills.

Pentest is not new to large corporations which have relatively high maturity posture. And it is also often mentioned and applied in meeting compliance and regulatory requirements such as *HKMA TM-E-1 Risk Management of E-banking v.3 Oct 2019, PCI DSS /GDPR Compliance, SFC Guideline on Cybersecurity for licensed corporations, eff. Jul 2018, Insurance Authority Guideline on Cybersecurity, eff. Jan 2020.*

Red teaming is a broader approach to Pentest. Red teaming's goal is to test the clients' detection and response capabilities as well as the overall robustness of their people, process and technology. We develop tactics, techniques and procedures.

OUR APPROACH

Methodology: Our Pentest builds on Open-Source Intelligence (OSINT) and Open-Source Web Application Security Project (OWASP). It involves a manual process supplemented with automated tools to identify vulnerabilities.

The Pentest phases include 1. Reconnaissance, 2. Scanning, 3. Vulnerability identification, 4. Exploitation and 5. Risk Analysis. Good testers are pragmatic. Our security consultant jumps around among the phases as discoveries warrant.

Coverage:

Tools used: Nessus Professional, Burp Suite Professional, and various open-source tools such as Kali Linux, Postman, MobSF.

Rules of Engagement: Before the start of the test, we define the scope, determine the primary concerns upfront and set limits on the depth of the test. Also, we discuss the level of communication required by project owner during the testing period, especially when critical vulnerabilities are discovered.

Deliverables: A professional report with detailed findings and a presentation of key findings.

Some examples of previous critical findings: A high risk vulnerability (not revealed by auto scanning) which may lead to DoS on Cisco WebVPN portal; Gained initial shell access by uploading Metasploit payload as attachment in a Website forum; Exploited SQL injection vulnerability in website leads to disclosure of CMS admin credential, Insecure Webcam devices pose privacy issues etc.

FAQs

Q1: What's the difference between Pentest and vulnerability scanning? Pentest applies manual effort to exploit the identified vulnerabilities and discover any unknown vulnerabilities. Vulnerability scanning uses automatic tools to discover known vulnerabilities.

Q2: What is the key factor to influence the number of findings for a Pentest? Besides the pentester's skill set, time is also a key factor. Time-limited engagements do not allow for a full evaluation of all security controls. Prioritizing the assessment would be required to identify the potential weakest security controls an attacker would exploit within a time constraint.

Q3: What are the risks of a Pentest? The potential risks may include data disclosure, system outage, traffic slowdown etc. However, with the rules of engagement, the pentest could be conducted in a more controllable manner to keep the risk at a minimal.

OUR PRINCIPAL CONSULTANT AND CYBERSECURITY CERTIFICATIONS

Mr. Freeman Ngai, our principal security consultant, is a co-founder of Pentastic Security Limited. Freeman has over 20 years of IT experience. His previous security projects cover companies in sectors like asset management, securities companies, legal/professional firms, manufacturing companies and the government. His core expertise includes Offensive Security, Email Technology and Reverse Engineering.

CISSP	CISA	OSCP	OSWP	GREM	CREST
Certified Information System Security Professional	Certified Information Systems Auditor	Offensive Security Certified Professional	Offensive Security Wireless Professional	GIAC Reverse Engineering Malware	CREST Registered Penetration Tester

Pentastic Security Limited is a category 4 *sub-contractor under the Standing Offer Agreement for Quality Professional Services 4.*

Contact:
Miranda Ma, Senior Business Development Manager
info@pentastic.hk +852 9168 0290

PENTASTIC
www.pentastic.hk

Updated as of 4 May 2021