PENETRATION TESTING

EFFECTIVELY CLOSE SECURITY GAPS

Our Penetration Testing is a full-service, multi-layered attack simulation orchestrated from the perspective of a malicious threat actor.

We design our tests to measure how prepared your People, Process and Technology are to withstand a cyber-attack from a real-life adversary, while uncovering potential risks, security vulnerabilities and configuration weaknesses.

Hedgehog's team of experts spend 3 months a year keeping their skills up to date, gaining deep understanding of the threat ecosystem, so they can test your business and identify your vulnerabilities, configuration weakness and gaps in protection to the highest quality.

We perform all types of Penetration Test including, but not limited to:

- API and Backend Systems
- Infrastructure – Internal, External & Cloud
- Mobile Applications – Android, iOS & Windows
- PCI-DSS
- Phishing – One off and regularly scheduled
- Physical
- Remote Access & VPN Systems
- Social Engineering
- Web Applications – from Blogs to Ecommerce

PENETRATION TESTING

Why is Penetration Testing important?

Penetration Testing is important for organisations of all sizes. A well-structured and scoped penetration test can help reduce the cyber risk exposure of an organisation as well as protect both the organisations and their client's data. It supports Data Protection compliance by evidencing regular testing (a GDPR requirement). Penetration Testing also assists with marketing. Once all the fixes are in place, the retest report can be a valuable marketing asset.

How we Penetration Test

A penetration test from Hedgehog will tell you not only what we found but how we found it. New vulnerabilities and exploits become available daily. We know, we help add to the volume by publishing vulnerabilities we identified and exploits we have created. Knowing how we find the issues is the key to your continual improvement, which is why we follow our 6 step high level methodology for every penetration test.

Pre-engagement	This is one of the most critical steps in ensuring success in your penetration test. The Pre-Engagement is where we work together to define the scope, and the goal of the test rigorously. We do this through a scoping call, and you can book these at a time and date convenient to you. During the scoping call for your penetration test, we are looking to identify exactly what needs testing, how complex it is and how much time we will need to use to complete the penetration test to the best of our capability. We will also look to identify the goal of the penetration test. The goal could be as simple as "identify all the exploitable vulnerabilities". It could be a lot more complex such as "pivot through an exploited host and attack the internal network to gain access to client data." Having a well defined scope is the key to the success of your penetration test. This is why we can never answer the question of "how much is a penetration test" until we have had a call to discuss your penetration testing scope.

Hedgehog Security Ltd.
Worklab, Europort, Gibraltar, GX11 1AA and
The Lab, Upper Tean, Stoke-on-Trent

Visit our website @ hedgehogsecurity.com
Call us on +350 540 73836 or +44 3333 444 256

PENETRATION TESTING

Intelligence Gathering

The second step in a penetration test is Intelligence Gathering, and it is a two-step process. The first step is, at Hedgehog anyway, done in the background normally a week before your test start date. Most of the intelligence gathering phase is performed by automated scripts. The scripts are typically used within a penetration test too, for more targeted needs. Essentially, we are looking to gather as much information about your business and your penetration test scope as we can from available public sources.

During the second part of the intelligence gathering phase, we will review the output from step 1 and any documents or information you have provided us. This is typically done the day prior to your penetration test starting. We will scour the internet, and to an extent, the dark webs, to identify any further information or data that could be beneficial to your test. The typical documentation we are looking for includes system architecture, data flow, infrastructure, concepts, password hashes, names, identities etc.

What is the purpose of this? Well, imagine if we were to find the company's internal information in a forgotten bit-bucket somewhere? This could be used in the penetration test to help gain access to systems. Equally, it will help identify any potential client information left exposed. It all goes to helping complete the most comprehensive penetration test available to you and ensure a positive return on your investment.

Reconnaissance

The reconnaissance phase of every penetration test builds on the Intelligence Gathering stage using active, in-depth technical review of the scoped environment. We will delve into each of the systems/applications in scope to identify the component structure and map all the points of interaction.

This part of penetration testing is vitally important to the success of the test. We will look to identify every point of interaction that a user can have with a system, application, or target. We will identify the technologies used and whether there are any easy wins that can be identified. This is done through port scanning, passive information analysis, mapping, and analysis. The goal if this phase is for our penetration testers to understand the scoped environment in its fully extent.

PENETRATION TESTING

Vulnerability Analysis

Vulnerability Analysis is the most time-consuming aspect of every penetration test. Vulnerability Analysis starts with a series of reviews of the scoped environment using various vulnerability scanning tools. We typically use several scanners and tools to aid in the rapid analysis of vulnerabilities. Our primary tool for vulnerability analysis is Secure, our in house developed vulnerability scanner. Secure uses several internally developed processes as well as commercial scanners including Nessus, OpenVAS and NeXpose.

The output from the vulnerability analysis phase is the identified of known vulnerabilities. Every one of these vulnerabilities is then manually reviewed and validated. Once the automated scans are complete and the vulnerabilities confirmed, the tester then moves on to attempting to find unknown vulnerabilities manually. With Web Application testing, the bulk of the time is spent in manual vulnerability analysis. Unknown vulnerabilities are commonly known as zero days, and these can exist in many different areas of the scope. Therefore, the vulnerability analysis is the most time consuming.

Exploitation

The exploitation phase of the penetration test is where we take all the vulnerabilities we have identified and use them to try and reach the goal set out in the Pre-Engagement step. We review each of the vulnerabilities, identify any exploits available for use and perform exploitation in a safe and controlled manner.

In a Web Application penetration test, this might lead us to bypass authentication controls or use other users accounts. We may be able to access information that would usually be protected by session management and authentication and authorisation controls.

In an Infrastructure pen test, this might result in the tester being able to sniff passwords on the network or gain access to a server. The goal of exploitation is to work towards achieving the objectives of the test incrementally.

Once an exploit is successful, the entire pen test process restarts at Intelligence Gathering within the context of the exploited system or application. Exploitation testing can be extremely time consuming so it must be conducted in a very controlled manner.

Post-exploitation

During the post-exploitation aspect of the penetration test, your pen tester will be analysing all the gathered data and the results of individual tests. The analysis includes categorising the detected vulnerabilities and prioritising them per the business and technical context. It is during this step that further testing needs are identified, and the tester will loop back and test or retest specific areas so that complete scope coverage is assured.

Hedgehog Security Ltd.
Worklab, Europort, Gibraltar, GX11 1AA and
The Lab, Upper Tean, Stoke-on-Trent

Visit our website @ hedgehogsecurity.com
Call us on +350 540 73836 or +44 3333 444 256