Hedgehog security

Why Perform Penetration Testing

There are a variety of reasons for performing a penetration test. One of the main reasons is to find vulnerabilities and fix them before an attacker does. Sometimes, the IT department is aware of reported vulnerabilities but they need an outside expert to officially report them so that management will approve the resources necessary to fix them. Having a second set of eyes check out a critical computer system is a good security practice. Testing a new system before it goes on-line is also a good idea.

Another reason for a penetration test is to give the IT department at the target company a chance to respond to an attack. The Payment Card Industry (PCI) Data Security Standard, and other recent security recommendations and regulations, require external security testing.

Finding Holes Before Someone Else Does

At any given time, attackers are employing any number of automated tools and network attacks looking for ways to penetrate systems. Only a handful of those people will have access to 0-day exploits, most will be using well known (and hence preventable) attacks and exploits. Penetration testing provides IT management with a view of their network from a malicious point of view. The goal is that the penetration tester will find ways into the network so that they can be fixed before someone with less than honourable intentions discovers the same holes.

In a sense, think of a Penetration Test as an annual medical physical. Even if you believe you are healthy, your physician will run a series of tests (some old and some new) to detect dangers that have not yet developed symptoms.

Discovering Gaps in Compliance

Using penetration testing as a means to identify gaps in compliance is a bit closer to auditing than true security engineering, but experienced penetration testers often breach a perimeter because someone did not get all the machines patched, or possibly because a non-compliant machine was put up “temporarily” and ended up becoming a critical resource. In today’s heavily regulated environment, many organizations are looking for better ways to continually assess their compliance posture. Most regulations have multiple components specifically related to system auditing and security.

What is Penetration Testing

Penetration testing is the common term used for attempting to gain access to information systems or assets without knowledge of identities, mechanisms or other normal means of access. In the past, Penetration Testing was focused solely Information Technology systems but now Penetration Testing is more holistic in manner.

The main differentiator between a penetration tester and an attacker is authorisation. A penetration tester will have authorisation from the owner of the assets that are being tested, always in writing from the client, and will be responsible to provide a report directly to the client. The goal of a penetration test is to increase the security of the assets being tested.

Often a penetration tester will be given base levels of access and in all cases, the goal would be to gain access to assets that the base level of access is not permitted. Within IT systems for example, this would be to elevate the status of the account or user via other means to gain access to additional information that a user of that level should not have access to.

In the majority of cases a penetration test is conducted to determine the level of assurance of security that can be given to an asset. As an example, a penetration test might be conducted against a new website freshly developed by a third party development company. In this example, a penetration tester would be expected to log and keep looking past the first hole so that additional vulnerabilities can be identified and fixed. It is important for the pen-tester to keep detailed notes about how the tests were done so that the results can be verified and so that any issues that were uncovered can be resolved.

It’s important to understand that it is very unlikely in a penetration test the penetration test team will find all the security issues. As an example, if a penetration test was done yesterday, the organisation may pass the test. However, today is Microsoft’s “patch Tuesday” and now there’s a brand new vulnerability in some web servers that were previously considered secure, and next month it will be something else.

Maintaining the security of your business assets requires constant vigilance.

Discover more

For further information call us on 0161 850 0454 or visit our website at https://www.hedgehogsecurity.co.uk and let us know we can help you move forward.

Reasons to Test

1. Identify Vulnerabilities
2. Discovering Gaps in Security
3. Discovering Gaps in Compliance
4. Security Training for your Staff
5. Verify Security Measures
6. Testing New Technology
7. Communicating Results

What We Can Test

- Buildings
- Infrastructure
- Vehicles, Boats, Planes
- Information Systems
- Mobile Applications
- Wireless Networks
- Traditional Networks
- Payment Systems
- Web Based Applications
- Near Field Communication Devices
- Electronic Devices
- Drones
- Wearable Devices

Bespoke testing can be tailored to your specific business requirements

Contact us:

T: 0161 850 0454
E: sales@hedgehogsecurity.co.uk
W: www.hedgehogsecurity.co.uk