CYBER SECURITY

PENETRATION TESTING

TAMARA
GLOBAL HOLDINGS 2016 LTD.

HTTPS://WWW.TAMARAGLOBAL.COM

WHY IS PENETRATION TESTING NECESSARY?

A secure system today doesn't mean a secure system tomorrow. With cyber attacks getting more and more prevalent in today's day and age it has never been more important to test your cyber controls. Penetration testing looks at vulnerabilities and will attempt to exploit them. The testing is stopped when the goal is achieved, the goal being when access is granted. This would confirm if the security controls you have in place are successful or not.

Organizations need to conduct regular testing of their systems for the following key reasons:

- To determine the weakness in the infrastructure (hardware), application (software) and people in order To develop controls
- To ensure controls have been implemented and are effective – this provides assurance to information security and senior management
- To test applications that are often the avenues of attack (Applications are built by people who can make mistakes despite best practices in software development)
- To discover new bugs in existing software (patches and updates can fix existing vulnerabilities but they can also introduce new vulnerabilities).

WHAT DOES A PENTEST CONSIST OF?

- Planning and data gathering—Define the goals of the penetration testing. Which systems will be included? What testing methods will be used? Gather data on the attack target, which may include the network or domain name, for example.
- Scanning—Tools are used to gather more data and information on the target. Example sinclude a vulnerability scanner and DAST tools, which are discussed in more detail in the next section.
- Gaining access—Web application attacks such as Cross-Site Scripting or SQL Injection are launched to expose vulnerabilities. Pen testers try to expose these vulnerabilities by stealing data or increasing permissions. The goal is to understand how much damage can be done.
- Maintaining access—Determine if the exposed vulnerability can be used to achieve a persistent presence in the application. In other words, can the attacker get deep within the web app, accessing sensitive data and causing more harm?
- Covering tracks—The attacker takes care to remain undetected. Changes made to the system must be returned to a state that will not raise a red flag.

Penetration testing results in a formal report that details the vulnerabilities that were exploited, how long the tester was able to remain undetected, and the sensitive data exposed. This information is used to remediate vulnerabilities and improve the security of the web application to help protect against real attacks in the future.

PENETRATION TESTING METHODS:

External testing—Only systems and assets that are visible on the internet, such as the web application itself, are targeted. The goal of the testing is to gain access to the application and its data.

Internal testing—The pen tester has access to the application behind the firewall. A potential scenario could be a rogue employee or stolen credentials from an employee.

Blind testing—The pen tester is given the name of the company, but nothing else. This simulates an actual application attack in real-time.

Double-blind testing—This is similar to a blind test, but the security team is not made aware of the simulation. They have no time to prepare for the attack.

Targeted testing—The penetration tester and security team work together, informing each other of steps taken to attack the application and to defend against the attack. This serves as a training exercise that provides real-time feedback during an attack.

Penetration testing is, for the most part, a manual process. Human testers need to apply a higher level of skill to properly identify all of the exploitable vulnerabilities in a web application.

HOW OFTEN SHOULD YOU CONDUCT A PENTEST?:

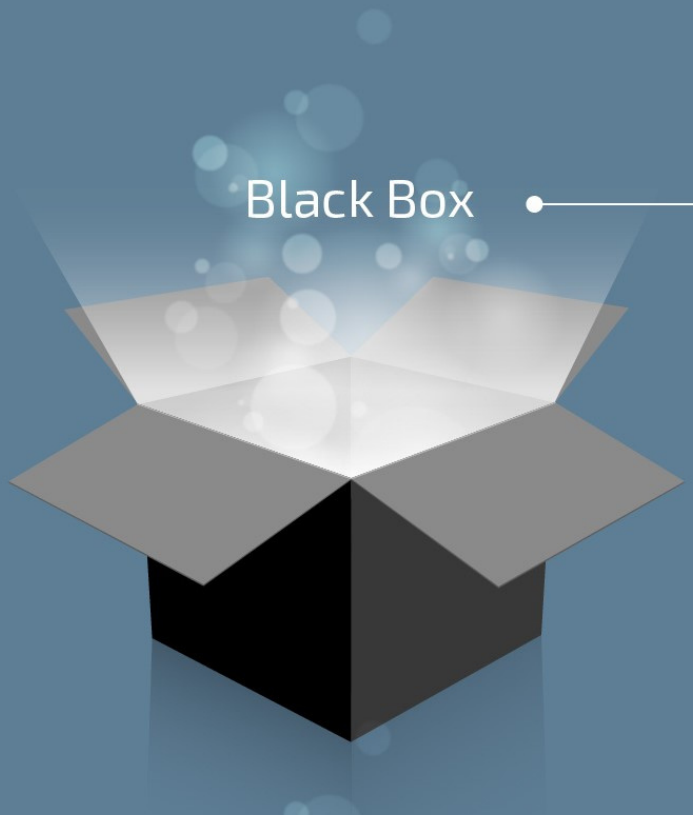
Pen testing should be conducted regularly, to detect recently discovered, previously unknown vulnerabilities. The minimum frequency depends on the type of testing being conducted and the target of the test. Testing should be at least annually, and maybe monthly for internal vulnerability scanning of workstations, standards such as the PCI DSS recommend intervals for various scan types.

Pen testing should be undertaken after deployment of new infrastructure and applications as well as after major changes to infrastructure and applications (e.g. changes to firewall rules, updating of firmware, patches and upgrades to software).

During the risk assessment, you will assess the impact of not complying to certain laws and regulations if you do not perform a penetration test on your products.

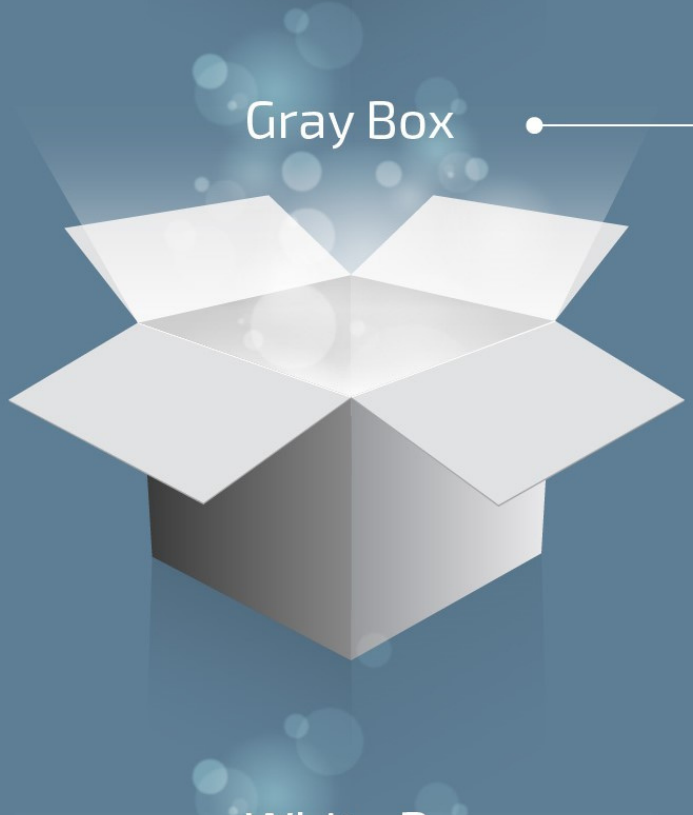
Non-compliance to regulations may cost you a hefty fine, lose you your license to operate, or even worse, get you jail time. Data privacy has been getting more attention and regulators from different countries are implementing strict data privacy laws to protect their citizens. It is important that you seek legal counsel to assess local laws and regulations and ensure that your company complies with those regulations.

Three Types of Pentesting



Black Box

before the pentest, a pentester receives minimum information about the target object from the customer, e.g., only an URL or IP address. This type of test is suitable for remote attacks simulation.



Gray Box

a pentester receives some information about the target object from the customer, and/or is granted some access to it, e. g., target object architecture and user access.

White Box

a security auditor receives full information about the target object with full access to it from the very beginning. E.g., the expert may be allowed to review the source code. This type of penetration testing brings the most results.

CONCLUSION

.

Penetration testing can help to mitigate the threats of the above risks that your business may face. However, good security practices should be adopted in order to secure your business. By taking a risk-based approach on cyber security, you will address the prioritized threats and review your business risk exposure continuously.


Headlines You DID NOT See
THE WALL STREET JOURNAL.
Government and Financial Websites Attacked and Taken Down; Stocks Show Concerns


The Daily Telegraph
Russia's cyber raiders foiled in humiliation for Putin


World NEWS
CYBER ATTACK


THE AGE
SUBSCRIBE
Crime syndicate hacks 15,000 medical files at Cabrini Hospital, demands ransom
A cyber crime syndicate has hacked and scrambled the medical files of about 15,000


theguardian
Met chief quits over hacking


METRO
CONNECT
YOUR GUIDE TO ALL THE WEEKEND FOOTBALL ACTION
MATCHZONE
Summer Sizzlers


DAILY EXPRESS
FREE ICE CREAM
NOW 20p
FREE LAVENDER PLANTS
NHS CHAOS AFTE
HACKER ATTACK
Patients hit as computer crooks demand ransom


THE TIMES
Dream family homes
500m web users hit by biggest hack in history
METRO
BAKE OF
DEAD AN
BERRY
UPGRADE

RUSSIA SPIES TRY TO STEAL OUR VACCINE


Daily Graphic
Chaos!
Enraged Awaso bauxite workers set buildings, vehicles ablaze


CYBER ATTACK
CYBER ATTACK
CYBER ATTACK


DAILY Mirror
PUPPY LOVE
Stars vow to end the cruel import trade


CORONAVIRUS
RUSSIANS T
TO STEAL
VACCINE SE
Putin spies accused of cyber attacks on UK labs


FINANCIAL POST
How Israel became a cybersecurity power — and what Canada can learn from it
The success has been fuelled by what one Israeli CEO described as 'an ecosystem that feeds itself'
Victor Ferreira
Apr 11, 2019 • Last Updated 1 month ago • 5 minute read


CYBER ATTACK
ATTACK
alamy stock photo


Hacking Brita
Cyber crime costs UK up to £27bn a year
44m
£18bn - £27bn
80pc
Top 4
£121bn
8pc


THE WORLD NEWS
CYBER ATTACK!


DAILY NEWS
CYBER ATTACK!