10 Reasons You Should be Pen-Testing

#1 Real World Experience

Penetration tests should be done without alerting the staff in order to learn whether the security controls you have in place actually work.

Think of it as a fire drill for your security measures. This way you can see if your security tools are working without the pain of an actual data breach.

#2 Train Developers

The results of your pen-test can help train developers to make fewer mistakes.

A penetration test picks out the backdoors, misconfigurations and other vulnerabilities in your network.

By using this information to train your developers, you can avoid these mistakes in the future and increase your security.

#3 Prioritize Your Risk

Now, a penetration testing tool can't do this on it's own. If you are pen-testing, as well as utilizing a vulnerability assessment tool, you'll find more meaning behind the data you uncover in your pen-tests.

Scanner data is great for telling you what vulnerabilities lie in your network and prioritizes your next actions. Without any prioritization, how would your team know which of these vulnerabilities to patch first?

With these two tools working together, you can see which of the vulnerabilities will have the greatest impact on your network – allowing you to prioritize your time and resources accordingly.

#4 Meeting Compliance

In the payment card industry, PCI-DSS regulations mandate both an annual and ongoing penetration tests – after any system changes.

While it is tempting to go with a lightweight pen-test service just to check the compliance block once a year or whenever mandated, think of it this way: if you are already going to allocate resources for a pen-test, why not get the one that will help you mitigate real risk?

#5 Uncover Holes in the Network

Penetration testing attacks your network like a hacker would and does whatever possible to breach.

This is a great reason to let a third party run a penetration test, even once or twice a year, to put fresh eyes on your network.

#6 Provide Evidence to Support Your Team

Provide evidence to support increased security investment or to prove the value of your current security tools.

We all know that time, money and resources are three things that we will never have enough of.

However, showing your leadership team the value in these solutions can help support your request for more resources or prove the value of your current team and solutions.

#7 Determine the Feasibility of Attack Vectors

We think we know how attackers would get into our system, however, with the results of a penetration test, you can have certainty in making your decisions or gather the information needed to spend your resources on a riskier attack vector.

#8 Post-Incident Analysis

After an organization has been breached, they need to determine the attack vectors used to gain entry to their system.

Combined with forensic analysis by your security operations team, penetration testing can re-create the attack chain in order to validate new security measures to prevent a similar attack in the future.

#9 Improve Security Response Time

Penetration testing is a real world hack on your system and should feel that way to your security team.

With penetration testing, you can not only find out the amount of time that it will take for an attacker to breach your system, it will tell you how prepared your security team is to remediate the threat.

#10 Bridge the Gap with Security Ops

As previously stated, attackers are coming at your system by any means possible.

In order to see not only how they get in, but where they can go once they get in, penetration testing can show you the lateral movement to help your team and your security ops team work together to block those paths.

Do we have your attention yet?

Penetration testing is essential to any security team. Wonder what this would look like in your network?

Request a customized demo and see what it would look like to pen-test your network, today!