Hop in the Ring with Penetration Testing

www.dmstechnology.com

The best way to learn how to defend yourself is to get attacked in the first place. It's the same logic that boxers utilize – and all other fighters, for that matter. Practicing with a punching bag is a good way to train, but it pales in comparison to training with a live person who can think, react, and outsmart your defenses.

The same is true for your network security. 75.6% of organizations encountered at least one successful cyber attack within the past 12 months.You can (and likely do) spend massive amounts of money preparing for cyber attacks by installing the latest software and hardware and running drills on theoretical attacks.

> "75.6% of organizations encountered at least one successful cyber attack within the past 12 months"
>
> **- CyberEdge Group**

But what good are those tools if they go untested and unproven? A boxer aims to train with a partner who will push them to their physical limit. They do this to learn two things. For starters, they learn where their own weak spots are so that they can address them. Secondly, they learn their opponent's fighting style. This makes them more likely to defeat them the next time they fight.

For boxers, this training is known as sparring. In network security, it's a practice called penetration testing.

Penetration testing consists of an active exploitation of weaknesses and security holes within an organization's network infrastructure. Usually, the testing will cover application security tests, application security tests, and tests to determine the effectiveness of internal controls and processes surrounding the network. Thorough penetration tests will include testing from both within and outside of the network.

Pick Your Sparring Partner

In a gym, you may not always want to choose the same partner to spar with. You'll quickly become accustomed to their attacks and defenses. The best way to improve your form is to train with a variety of fighters that each provide their own unique styles.

For penetration testing, the different sparring partners come in three different forms. They include black, white, and gray box testing. Each one will provide you with distinct pros and cons.

Black Box

In this scenario, you'll go up against an opponent who has zero previous knowledge of your systems and architecture. The "friendly hacker" will attempt to monitor your systems and learn as much about them as possible. They will launch a brute-force attack on your systems, hoping to find a vulnerability somewhere. This method is known as the trial-and-error approach.

Pros

» Most accurate representation of a random attacker attempting to access your systems

» Provides you with a thorough knowledge of your system's overall external security

» "Friendly hacker" doesn't require previous programming knowledge, making it less costly (due to not needing a highly skilled technician)

Cons

» Doesn't account for internal network attacks

» Takes the longest of the three to conduct, as the attacker will need to guess their way into your systems

White Box

This is the opposite of the black box testing approach. Your attacker will have comprehensive knowledge of your systems. These include how your architecture is structured, IP ranges, what device make and models you are utilizing, and more. This approach accurately simulates an attack by a knowledgeable internal source.

Pros

» Since the attacker has all of your information, the attack doesn't take long to complete

» Provides a complete attack scan that accounts for true vulnerabilities within your systems

» Time-efficient in finding security holes

Cons

» Since it requires a high level of attacker comprehension and IT knowledge, the costs are higher than the other two scenarios

» Requires access to code within the network, which can be troublesome to obtain

Gray Box

This test is a mix of both the black box and white box tests. It means that you provide the attacker with some basic knowledge of your systems and generally point them in the right direction. This scenario is the most realistic simulation of someone gaining a rudimentary knowledge of your systems and then attempting to break into them.

Pros

» With both known and unknown fronts being attacked, this method usually exposes the most prominent security flaws

» For the amount of flaws that it finds, it is extremely cost-effective

Cons

» Doesn't fully commit to one way of scanning for holes, so it won't work for finding deeply specific flaws in an internal or external environment

» Lack of access to code means that the attacker will not find developer-specific flaws.

Penetration Testing with DMS Technology

The best way to defend against cyber threats is to spar with the "friendly hackers." By finding the holes in your security, you'll be able to properly close them and defend yourself against an actual attack. And with cyber crime damage costs projected to hit $6 trillion annually by 2021, it's more critical than ever to have an airtight defense in place.

To properly prepare for the fights ahead, you'll want a sparring partner by your side that will push your network to its limits. They'll need to be knowledgeable, professional, and dedicated to helping you defeat any cyber threat that comes your way. With DMS Technology as your penetration testing specialist and partner, your network will be more protected than ever before. We'll work with you to choose the test that best fits your company's needs.

Ready to take your network security to the next level? Contact us today.

New York Office

780 Third Ave, 15th Fl
New York, NY 10017
United States

P: 212-561-5222
www.dmstechnology.com

London Office

Berkeley Square House, 2nd Floor
Berkeley Square, London W1J 6BD
United Kingdom

P: 0207-084-7155
www.dmstechnology.com