

Penetration Testing

"Black Hats" and "White Hats"

In the network security world, there are two main categories of people. Black Hats and White Hats. Black hats are considered the hackers who try to gain knowledge of your network, compromise that network, stop the network from performing services and try to steal data from the network. White hats are equally skilled individuals that try to protect networks and prevent the black hats from their goal. In penetration testing, the project can be conducted in one of two ways: Using a black hat approach or a white hat approach. The black hats normally have very limited knowledge of your internal network and systems and are usually attacking your network blind. So when we simulate this approach, little information is giving to the testers and they must spend time and effort to gain knowledge of your network. White hats are defending your network and usually have some knowledge of your internal network and systems. So when we simulate this type of attack, information regarding the internal network and systems is disclosed to the testers before testing. As you might expect, there are conflicting opinions about this choice and the value that either approach will bring to a project.

Some penetration testing organizations will suggest that when given the choice, the black hat approach is the best because it closely simulates the process of a real hacker. This theory is not always true and the safest approach. Firstly it presupposes that an attacker doesn't have any knowledge of your systems, which is actually unlikely. If someone is targeting your organization specifically then it is a strong possibility that they do indeed have detailed knowledge of your systems and procedures (an ex-employee with a grudge for example). In which case it would be wise to assume the worst, that they in fact have complete knowledge of your systems. If your security relies solely on the secrecy of your designs, then you do not have any tangible security at all. Secondly, a hacker will not be limited to any time constraints that might be applied to a penetration test. For arguments sake, they will not have a week in which to circumvent your security measures, they will happily be able to probe away for years (if undiscovered) until they find a weakness they can exploit.

There is also the question of value for money. In conducting a black hat test it is necessary to spend a reasonable proportion of the time allocated for the project on discovering the nature of the infrastructure and how it connects and interrelates. Obviously, if the time is being spent on discovery, it is not being spent on actually testing for vulnerabilities.

This is not to say that black hat testing has no value, it does. It is useful for finding out how information leaks from your systems that might be utilized by others (such as in mail headers). When choosing a black hat test it just needs to be born in mind that to get the same amount of time spent on accessing vulnerabilities, you will need to allocate more time overall to the project.