Closing the Door on Network Attacks

by Barron Rosborough, 8/17/18 1:26 PM

Network security scanning

Your network is 100 times more likely to be attacked with a known exploit than an unknown one. And the reason behind this is simple: There are so many known exploits and the complexity of networks is so great that the chances are good that one of these known vulnerabilities are present and will allow an attacker access to your data.

The number of networks worldwide is so great and the number of new, as of yet undocumented and thus unknown exploits so small that your chances of being attacked with one is nearly zero - unless you have network assets of truly great value, or you are a particularly interesting target.

If you don't attract the attention of a dedicated, well financed attack, then your primary concern must be to eliminate your known vulnerabilities so that a quick look would not reveal an easy entry.

Network security defense strategy

There are two roads to accomplish excellent security. On one you would assign all of the resources needed to maintain constant alert to new security issues. You would ensure that all patches and updates are done at once, have all of your existing applications reviewed for correct security, ensure that only security knowledgeable programmers do work on your applications and have their work checked carefully by security professionals. You would also maintain a fiendishly restrictive firewall, antivirus and IPS/IDS.

Your other option: use a security scanning solution to test your existing equipment, applications and web site to see if a KNOWN vulnerability actually exists. While firewalls, antivirus and IPS/IDS are all important, it is simple logic to also fix the very issues that hackers are looking for. It is more effective to repair relatively few actual risks than it is to build higher and higher walls around them. Network vulnerability scanning is the most efficient security investment.

If one had to enough resources to take just one of these roads, diligent wall building or vulnerability management, it has been demonstrated that fixing vulnerabilities instead of building walls around them will produce a higher level of security on a dollar for dollar basis. This is proven by the number of well defended corporate and government networks which get hacked every month.

Network security using a security scanner

Your best defense against an attack on your network is to regularly scan it, fix the high risk vulnerabilities the scan finds.

Beyond Security staff have been accumulating a library of known issues for many years and have compiled what is arguably the world's most complete database of security vulnerabilities. Each kind of exploit has a known combination of network weaknesses that must be present to be accomplished.

In a matter of hours, a security scanner can run through its entire database of over ten thousand vulnerabilities and can report on which are present and better yet, confirm the thousands that are not. With that data in hand you and your staff can address your actual security vulnerabilities and know that your network is completely free of known issues.

Then security scanning can be run on a regular basis so that your network will be tested against new vulnerabilities as they become known and provide you with solid data as to whether action is vital or low priority. You will also be alerted if new equipment has been added, a new port has been opened that was unexpected, or a new service has been loaded and started that may present an opportunity to break in.

In complex, large systems it may be that weekly scanning is the ONLY way to ensure that none of the many changes made to equipment or applications may have created a weakness that a determined hacker could exploit.