Barron Rosborough, 9/14/18 11:31 AM

# Why VM got a bad rap

The number of servers, desktops, laptops, phones and personal devices accessing network data is constantly growing. The number of applications in use grows nearly exponentially. And as known vulnerabilities grew in number, IT managers found that traditional vulnerability management tools could easily find more problems than could be fixed with their existing budgets.

One solution to the problem of having known, unfixed weaknesses on internal hosts has been to concentrate on building better walls around the network to keep attackers from accessing the weaknesses. Vulnerabilities have been addressed when and if there are resources available and sometimes never.

Other solutions are to either scan just the most important network resources, or to prioritize the vulnerabilities so that limited resources could be applied to fixing just those that were most likely to be attacked or be the source of data loss.

None of these solutions are working very well. Even random and unfocused attackers are routinely bypassing antivirus, firewall and IPS to find and exploit the vulnerabilities on secondary systems or hosts that were left unrepaired because they weren't high risk. After gaining a foothold there hackers have then moved deeper into the network and walked away with the good stuff.

The vast majority of successful attacks are on the most well known, easily discovered and easily exploited vulnerabilities. Most attackers study up on a specific vulnerability then search broadly for any network that has that weakness and then they exploit it to gain access. From that beachhead they expand their control through the network and then look for the valuable data they can steal without being discovered.

## Is the use of vulnerability management tools an art?

Vulnerability management tools fell from grace because they failed on two fronts. Their reports have been riddled with errors and their vendors got into a race of who could find the most vulnerabilities. VM reports became so thick as to be un-usable.

If pockets were deep and resources unlimited then every vulnerability found by a traditional vulnerability management tool could be validated and then fixed. In the real world nobody had that much time or money. And so the decade of building better walls was launched. It's called the layered approach to security and it's not working.

And now we are faced with running multiple, complex systems that overlap and disagree with each other and don't seem to be keeping the attackers out.

It boils down to not having the right vulnerability management tool and not having the head count to do the real work needed. We propose that the solution is to revisit your vulnerability assessment tools, but this time focus on accuracy and usability.

## "Closing the door." - Dealing with known vulnerabilities

Almost all attacks are accomplished using known vulnerabilities. Even Stuxnet utilized a blend of known and 0-day vulnerabilities and would have been severely limited in its scope had there been no known and unresolved vulnerabilities in the networks it attacked. So, making sure that every server, every workstation and every device is up-to-date with the latest security patches is the solution to the out of control complexity of network security.

Unfortunately this is not so simple. Many organizations need to deal with thousands of network assets and small networks often have hundreds. Even if vulnerability management tools have been used to put every Microsoft patch in place, there are still devices and applications in your network from dozens of other vendors. Many are not good at patching problems rapidly. Moreover, most networks have accumulated applications and code that are no longer in production but are kept around, just in case. If these are not actively tested and patched or removed, then these offer an easy avenue for entry to your system.

A vulnerability management tool such as beSOURCE, the automated vulnerability detection system, automates this process by identifying all the known vulnerabilities in your network and prioritizing them based on the importance of the asset and the criticality level of the vulnerability. With vulnerability management you can gain certainty that your limited resources are being applied to the most serious network issues.

## Vulnerability management tools & behavior analysis

You have limited resources and can't afford to chase vulnerabilities that don't exist or miss fixing something really important.

Most Vulnerability Management tools rely primarily on checking application banners to read the version number. They then assume that if version X is present, then all the vulnerabilities of version X are also present. This can be false for a number of reasons including 'back-doored' updates (common in Linux) or if server or application settings make access to the vulnerability impossible.

Most vulnerability management tools assume that if a host displays the most current version, then it is free of vulnerabilities. This too may not be the case as a patch may

not have completely installed or a machine may not have rebooted, leaving the patches incomplete.

beSOURCE applies behavior analysis to vulnerability management. It delivers specially crafted queries and uses the resulting behavior of network components and web applications as its primary indicator of whether a specific vulnerability exists or not. This means that beSOURCE is extremely accurate, generating nearly zero false positives and it finds vulnerabilities that other solutions cannot identify (false negatives).

## beSOURCE for any vulnerability management need

beSOURCE is available for networks of any size and using appliance, hosted and hybrid implementations. It can scan a just a few web sites, or manage a large, widely distributed network that extends across hundreds of business units or multiple continents. Flexible licensing and great support make it a common sense solution to any vulnerability management tool requirement.

For more information, please call, email or visit: www.sekureit.net

.