CSO
FROM IDG
July 08, 2019 www.csoonline.com

REVIEW

Review: XM Cyber HaXM makes automated penetration testing more accessible, reliable

HaXM is the next logical evolution of automated pentesting programs. Not only does it offer continuous scanning that is easy to configure, it also provides advice to help fix problems.

By John Breeden II

Enterprise networks are amazingly complex these days, to the point where one misconfiguration can potentially expose an entire organization to dangerous vulnerabilities and attacks. To find those problems before a hacker could uncover them, cybersecurity teams traditionally conduct so-called red team exercises where trained attackers would try to compromise a network and then report their findings. But those exercises are likely too infrequent in today's world of constantly-changing configurations, cloud computing and even software-defined networking.

To fill that gap, many cybersecurity firms developed penetration testing tools that are supposed to be able to perform the job of a red team at any time. We've reviewed several on CSO. All of them we evaluated were good at what they did, but most required at least some knowledge of the kinds of vulnerabilities users wanted to scan for, and few offered to help fix the problems that they discovered.

The HaXM program from XM Cyber aims to make automated penetration testing more reliable and accessible by improving on the current state of similar programs in several ways. First, HaXM does not require any knowledge of attack techniques. For example, you don't have to scan for a specific code injection vulnerability on a web server. You simply need to tell the program that the web server is an important asset in your network and then let HaXM discover all the ways that it could be compromised. Second, HaXM offers continuous scanning, so results are never aged out over time. And finally, in addition to performing red team type exercises, HaXM offers detailed advice on how to fix problems it discovers and which ones should be fixed first, effectively taking on the role of a so-called blue team in security exercises.

Getting started

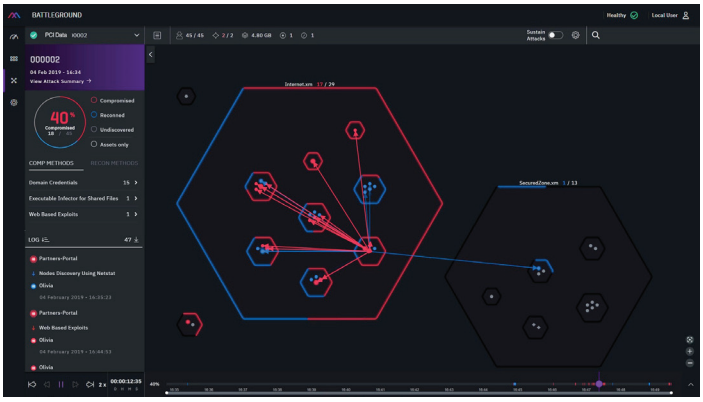
Installing XM Cyber's HaXM is a relatively simple process. There is a main server that houses the brains of the program. It can be deployed locally for extremely security-conscious organizations or it can be accessed through the cloud in a software as a service model. And then there are the software agents, which are extremely lightweight, and need to be installed on every critical asset you want HaXM to protect. The agents allow the program to run simulated attacks against those assets.

Pricing for HaXM is based on a yearly subscription model that scales up based on how many endpoints an organization owns overall. However, users can have as many agents as they want deployed on critical assets, and adding more does not affect the pricing.

Setting up HaXM isn't complicated, though it is normally done with the help of XM Cyber as part of the yearly subscription cost. Most of the setup time involves defining the critical assets that the program will protect, deploying agents, and then telling the program what security questions you need it to answer. For example, you might ask, "Can my database be accessed by unauthorized users?" or "Could an attacker use other exploits in order to move laterally to the server?" This will generate several tests that can be set to keep running over a certain period of time, anything from minutes to days or weeks. Tests can also be set to repeat at regular intervals.

Testing HaXM

Once an attack runs, users are given a report, which is accessed through the main HaXM server. HaXM can be configured to alert a

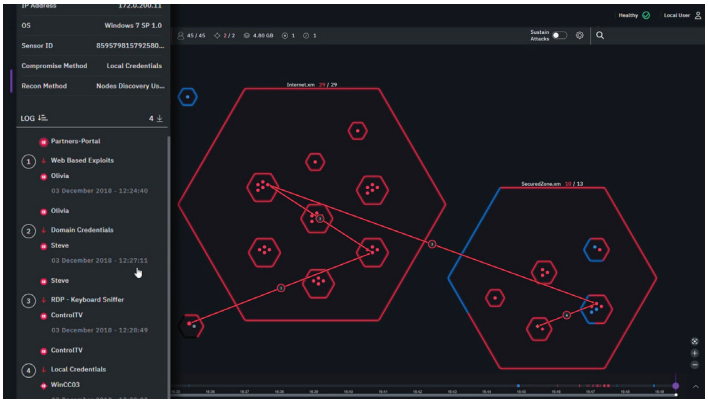


CSO

Once a critical asset is breached, users can see all of the paths taken by the simulated hacker, the vulnerabilities exploited along the way, and even which users could be used to further the attack. This is all done using real data from the network that HaXM is protecting.

security information and event manager (SIEM) about the results of a scan, but users still need to look at the actual report through the main interface. The attack report screen is called The Battleground; it looks a bit like one of those wargaming combat maps with hexagons representing different network assets and diamonds representing the critical assets (i.e., the crown jewels) that the program is trying to protect.

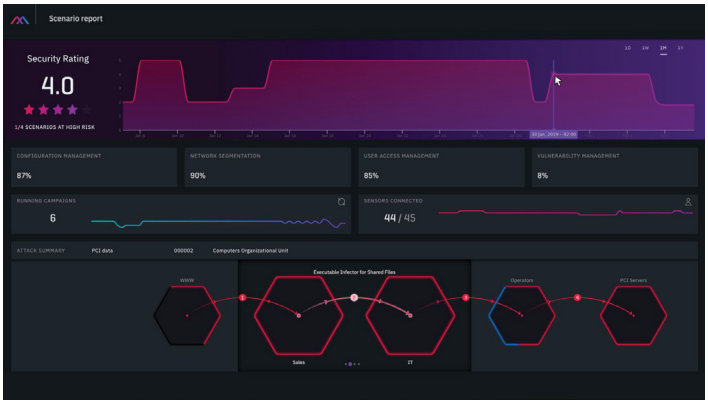
The attack simulation is represented by a series of arrows that slowly shoot from asset to asset, turning it from blue to red if it would be comprised by a real attack using a particular technique. The simulation plays out graphically like a movie in real time, with play, fast forward, rewind and pause buttons at the bottom of the screen to control it. In our first test, a critical server was compromised in just over three minutes, and it was fascinating to see how a real hacker might accomplish that feat.



CSO

The XM Cyber HaXM attack simulation can be displayed in movie-like fashion in the battleground section of the program. Controls are used to fast forward or rewind to important parts of an attack once the test is complete.

Each element of the simulated attack contains very detailed information about how an attack could compromise real network assets. In another test, a webserver was compromised en route to a better target, but the simulated hacker had to wait until a real user with an unpatched and vulnerable browser visited it to perform any further lateral movement. If that did not happen during the duration of the test, which can be set to days or even longer, then HaXM would not be able to capitalize on that particular vulnerability, though it would try other things in the meantime.

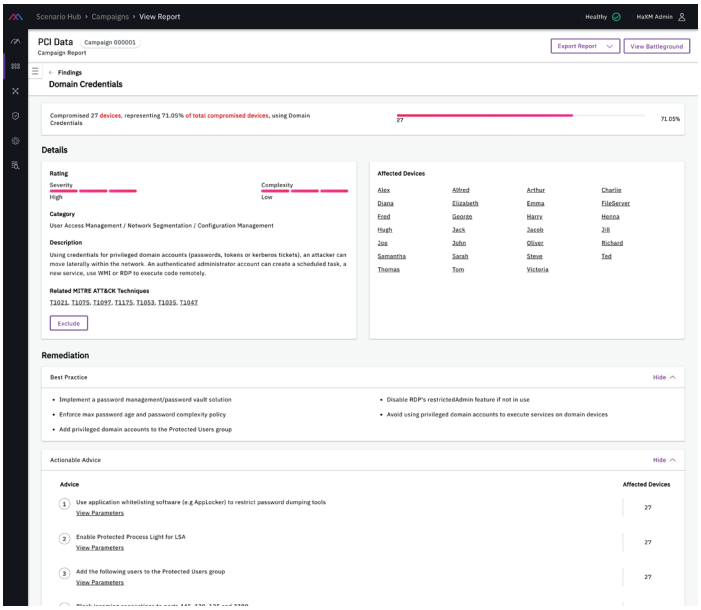


CSO

While the true value of the program is in the individual reports, HaXM also has a graphical dashboard that can alert users whenever scans uncover critical vulnerabilities.

Once a test is complete, HaXM ranks the vulnerabilities that it discovers. Factored into the ranking are things like how easy it would be for an attacker to exploit the discovered problems, how easy it would be to craft a fix, and how badly critical assets could be compromised. That way, security teams can work on the most critical problems with the easiest fixes first. Many of the problems discovered by HaXM on the test network were based on configuration errors, which is no wonder given how complex networks are these days. An overall report covering every scan and problem detected by the program is also always available through the main HaXM dashboard.

In addition to simply ranking what it finds, HaXM also provides actionable advice about the best way to fix problems so that future simulations, and real hackers, can no longer use the paths discovered by the scan to compromise a critical asset. The advice is written very sensibly, and suggests things like not storing credentials in a cache file after use. It also explains how to accomplish those fixes, which for the example above would be to add administrators and other privileged users to the protected users group for Windows networks. To check if the blue-team fixes are effective, simply trigger another scan.



CSO

In addition to just pointing out vulnerabilities and putting them in the context of a simulated attack, XM Cyber HaXM makes recommendations about how to fix the problems, and which ones need to be addressed first.

The last word

The XM Cyber HaXM program is the next logical evolution of automated penetration testing programs. Not only does it offer continuous scanning that is easy to configure, even for junior cybersecurity analysts, but adds advice to help fix problems. This makes it a very complete and highly useful package for finding and fixing whatever paths hackers might use to breach a highly complicated network's defenses.