Scanning Your Cloud Environment

LEAD

The “cloud” is a reality for IT professionals, but how secure is it? Since Cloud Service Providers (CSPs) do not allow cloud consumers to individually test their environments why not use a third party Vulnerability Assessment Scanner (VAS) tool/service? Read on to gain an understanding of what third party VAS tools/services are available to cloud consumers, what cloud platforms these services are associated with, their pros and cons, how to use these tools, and what to look for in the future with testing the security of your cloud environment.

INTRODUCTION

The security of an organization’s data, network, and systems in the cloud are a relevant concern. To alleviate this concern CSPs have partnered with third parties to allow these entities to independently test their environment. These third parties, like CORE’s CloudInspect and McAfee’s Database Security Scanner (DSS) have an offering, but how reliable are they, how much do they cost, what are the pros and cons with using one versus another, and what does the future hold for this market?

BODY

Amazon’s Web Services (AWS) group offers a third party service called CloudInspect for their clients/customers to test the security of their environments for an additional fee. This service has recently been brought to market due to regulatory compliance and/or contractual (e.g. PCI DSS) requirements from both sides of the equation, namely AWS and its consumers/customers. CloudInspect is a full-blown vulnerability assessment tool that scans for vulnerabilities associated with the Operating System (OS), configured services, and the (web) application environment. To start a scan using CloudInspect the user must create an account, enter their AWS keys, and then choose a running AWS instance (see below).

Figure 1: CloudInspect AWS Instance Selection
This feature simplifies the discovery of the available instances on AWS, and as time goes on it is hoped that as CORE adds additional CSPs partners that this interface would show all available/operational instances as a dashboard for scanning.

After the user chooses the instance to run a scan on, there is a prompt for the URL to scan, which is reminiscent of other vulnerability assessment tools in the market like Nessus, OpenVAS, and Acunetix. After the instance and URL are chosen the scan is started, and like other tools, CloudInspect has a very intuitive dashboard for checking on the status of the scan.

Figure 2: CloudInspect AWS Scan Results

Beyond the status of the scan, CloudInspect does a very nice job of breaking down the results into various reports, with a description on the premise of each report (see below).
CORE’s tool provides an easy, intuitive interface; however, there are concerns about the depth and breadth of the scan. Our scan focused on the phpMyAdmin implementation on our large Elastic Compute Cloud (EC2), AWS LAMP (Linux, Apache, MySQL, and PHP) instance using Amazon’s Machine Image (AMI) Linux-based OS, and zero vulnerabilities were found. As we have not patched/updated that machine recently and/or hardened it (e.g. strong passwords, strong access controls, proper firewall settings, proper PHP settings, checking for a running anti-virus application with an updated virus signature) from a security standpoint, the lack of findings is a concern. In defense of CORE’s product, we set the URL to the phpMyAdmin implementation, which means that we configured the scan to run like a Web Vulnerability Scanner (WVS) versus a VAS. However, it is felt that either there is an obfuscated scanning surface for the AWS platform, an inability to inspect the virtual layer of this environment, or that CloudInspect does not scan to an acceptable level of detail for the cloud environment. Ultimately, it is felt that a better description of the tool/service will establish a proper expectation from the user.

With its faults, CoreInspect is currently cost-effective at $20 per scanned machine instance/web application, though it is believed that the cost of CoreInspect will rise as the service improves. Furthermore, it should be noted that Amazon does not allow their small or micro instances to be scanned because of resource limitations. There are other options other than CloudInspect for scanning cloud instances, to include McAfee’s DSS offering.

From a database perspective, Microsoft’s SQL Azure has been added as an optional scanning platform for McAfee’s DSS, which was formerly known as Sentrigo’s Repscan. This local, thick-client application is the only product/service available today that includes the ability to scan a cloud-based database platform. As this tool solely includes SQL Azure at the moment it will be interesting to see if McAfee and AWS decide to engage in a business relationship, namely the ability to scan AWS’s Relational Database Service (RDS) and/or AWS’s Distributed
Database System (DDS) offering, called SimpleDB. Or, it may be Oracle who decides to allow McAfee to scan its current Database Cloud Service. Time will tell.

DSS is reminiscent of several database-focused Integrated Development Environment (IDE) toolsets on the market today, namely RazorSQL, SQL Developer, and/or Toad where one can select from a collection of supported databases to connect to (see below).

![Database Selection](image)

Figure 4: DSS Database Selection

After the user enters the connection information, s/he is presented with a checklist of specific focal points that the scan should cater towards, which is a great piece of functionality given that most scanning efforts these days are to attest and/or certify compliance (see below).
It should be noted that, like CloudInspect, DSS did not find many vulnerabilities, which (like AWS) may hint towards either an obfuscated scanning surface for the SQL Azure platform, an inability to inspect the virtual layer of this environment or that DSS does not scan to an acceptable level of detail for the cloud environment. However, like CloudInspect, DSS provides intuitive, aesthetically pleasing reports and results to look at (see below).
McAfee’s pricing for the DSS offering is dependent on the use of Value-Added Resellers (VAR), though the cost hovers somewhere around $2,000.00 per year for vulnerability definition updates. The value-add for this product line is that it is equally useful for on-site database instances as it is for cloud instances. Due to the ability to use this tool for both deployment models, McAfee’s DSS will have an enhanced Return on Investment (ROI).

Speaking of ROI, one may ask about the existing on-premise VAS providers and their ability to deliver a service to scan a cloud environment, as many enterprises have existing investments with these tools. It is inevitable that these vendors will incorporate the ability to scan cloud instances, though the question will be what products align with what CSPs, and how effective they are at scanning cloud environments. Time will tell who will align with whom, but names like Tenable (offering Nessus), Qualys, and IBM (offering AppScan) come to mind as vendors who will eventually partner with a CSP.

While on the subject of CSPs aligning with on-premise scanning vendors the thought comes to mind of whether or not the CSPs will offer scanning services themselves. Furthermore, if CSP-offered scanning becomes commonplace the question then becomes do these vendors build such a product organically, or acquire one? A driver for CSP offered scanning could be if the currently offered tools/services on the market continue to have difficulty scanning virtual environments. Though McAfee’s DSS and CORE’s CloudInspect have an intuitive interface and reports, they both have shown questionable results, but for the time being they are the only options to scanning your cloud environment.

CONCLUSION

The pickings are pretty slim for tools/services to scan your cloud environment, and the results shown with the existing tools are questionable; however, this is what is available and their interfaces and reports are intuitive. In time, the market will offer additional tools/services (e.g. a
Scan Authorize Application Programming Interface, ScanAuth API) and it is to be determined whether these tools/services will enable an enterprise to use its existing scanning investments, and thus achieve a higher ROI, or if the CSPs will offer these tools/services. Regardless, tools to scan your virtual environment are in their infancy, and the accuracy of scanning a virtual environment will be a determining factor for the cloud VAS landscape.

In the meantime, consumers only have McAfee’s DSS and CORE’s CloudInspect available to choose from, and as shown these tools/services are fairly easy to learn and are cost effective. As the cloud grows out of its infancy to reach critical mass, as security products learn to handle virtual environments, and as organizations strive to find cost efficiencies, this market will grow. Until then, use this article in conjunction with CloudInspect and DSS to assess your external cloud environment.
Biography

Steve Markey is the Principal of nControl, a consulting firm based in Philadelphia, Pennsylvania. He is also an Adjunct Professor, and he is the current president of the Delaware Valley (Greater Philadelphia) chapter of the Cloud Security Alliance (CSA). Steve holds multiple certifications, degrees, and has over eleven (11) years of experience in the technology sector. He frequently presents on: information security, information privacy, cloud computing, project management, eDiscovery, and information governance.