DABomb
RiskSense’s Automated Exploitation Framework
# Table of Contents

Executive Summary 1  
Introduction 2  
The Problem: Repetitive Penetration Testing Tasks Decrease Efficiency 2  
The Solution: RiskSense-Developed Tool, DABomb, Increases Penetration Testing Efficiency 2  
DABomb: Three Features to Increase Efficiency 3  
  Scanning 3  
  Exploitation 3  
  Post-Exploitation 3  
DABomb: How Does this Artificial Intelligence-Based Automated Exploitation Framework Optimize Tasks? 4  
Moving Forward: Bringing DABomb to RiskSense’s Clients 4  
  Additional Deployments 4  
  Web Interface 4  
  Remote Functionality 5  
  More Integration Options 5  
    More Tools 5  
    KOADIC Integration 5  
DABomb: Bringing Cost-Effective Benefits to Organizations 6
Executive Summary

RiskSense Attack Surface Validation helps identify and prioritize threats, providing clients with immediate results and allowing them to secure their business and assets. RiskSense’s services are geared to identify potential attack paths where layered vulnerabilities across diverse technologies allows for progressive business exposure.

Known attack techniques are time-consuming to reproduce; RiskSense has the only AI-assisted penetration testing service that expedites this process. RiskSense experts and their discipline for attack surface testing led to the creation and sharing of open-source code to the security community that rapidly replicates sophisticated post-exploitation techniques across large scale networks. These unique tools allow RiskSense to focus more on the sophisticated attack vectors that may be present in their IT infrastructure and deliver greater value with RiskSense Attack Surface Validation services.

One challenge that security analysts face when conducting penetration tests includes optimizing their testing capabilities in a limited testing window. When conducting penetration tests, security analysts spend a significant amount of time repeating the same steps to complete their assessments. Because of this, analysts are often forced to skip various testing methods due to resource and time constraints.

It would be a dream come true, especially for penetration testers and security analysts, if some of these repetitive steps could be automated. This is a perfect example where AI and interactive learning can help with automation and bridge the human-machine divide.

After several successful tests, RiskSense started constructing a tool that could quickly complete repetitive tasks during a penetration test. That gave birth to a solution called DABomb.

DABomb is short for Domain Administrator Bomb and is a state-of-the-art, all-in-one automated framework for scanning, exploitation, and post-exploitation. DABomb is unique in that it automates repeatable penetration test exploit techniques, enabling security analysts to report effectively on results that are generally easy to obtain but are time-consuming to process.

DABomb is an incredibly versatile tool that RiskSense continues to improve. Benjamin Mixon-Baca and Daniel Peterson, two of RiskSense’s prototype developers, have worked hard to enhance DABomb’s functionality. These enhancements include future deployments, a web interface, remote functionality, and additional integration options, including integration with another RiskSense-developed tool, KOADIC™ C3 (COM Command and Control).

DABomb is a powerful tool that improves customer satisfaction and generates cost savings by increasing efficiency and reducing penetration test cycle-time. DABomb provides security analysts the power to optimize their penetration tests through automation, allowing them to focus on complex tasks that require human interface.
Introduction

RiskSense Attack Surface Validation helps identify and prioritize threats, providing clients with immediate results and allowing them to secure their business and assets. RiskSense Attack Surface Validation discovers the vulnerabilities most likely to be used by cyber adversaries to infiltrate and exploit organizations.

Discovering vulnerabilities is not enough, especially for complex environments. RiskSense’s services are geared to identify potential attack paths where layered vulnerabilities across diverse technologies allows for progressive business exposure.

Known attack techniques are time-consuming to reproduce; RiskSense has the only AI-assisted penetration testing service that expedites this process. Also, RiskSense experts and their discipline for attack surface testing led to the creation and sharing of open-source code to the security community that rapidly replicates sophisticated post-exploitation techniques across large scale networks.

These unique tools allow RiskSense to focus more on the sophisticated attack vectors that may be present in their IT infrastructure and deliver greater value with RiskSense Attack Surface Validation services.

The Problem: Repetitive Penetration Testing Tasks Decrease Efficiency

With so many tools at their disposal, security analysts have numerous options in determining how they conduct penetration tests. Security analysts have the option of using various open-source tools, their own programs, and commercial software to conduct these assessments. Having so many options sounds great in theory; however, security analysts are often limited in what types of activities they can conduct during the limited time frame of an assessment.

When conducting penetration tests, security analysts spend a significant amount of time frequently repeating the same steps to complete their assessments. Oftentimes, security analysts are forced to skip various testing methods due to manpower and resource constraints. Many of these steps are easy to complete on a small scale; however, on larger assessments, these small steps start to consume valuable time.

After several successful tests, RiskSense started constructing a tool that could quickly complete repetitive tasks during a penetration test. This tool is known as DABomb.

The Solution: RiskSense-Developed Tool, DABomb, Increases Penetration Testing Efficiency

DABomb is short for Domain Administrator Bomb and is a state-of-the-art, all-in-one automated framework for scanning, exploitation, and post-exploitation. DABomb is unique in that it automates repeatable penetration test exploit techniques, enabling security analysts to report effectively on results that are generally easy to obtain but are time-consuming to process. DABomb incorporates numerous open-source tools and gives these tools the ability to work together without extensive manual manipulation.
Scanning
The scanning phase of a penetration test involves the security analyst using the tools at their disposal to gather the target’s vulnerability information. During this phase, host enumeration on the network and vulnerability discovery on the active hosts provide security analysts with the information they need to prioritize their attacks.

DABomb allows security analysts to automate the scanning process to find the intersection of both the most common vulnerabilities and the most easy-to-exploit vulnerabilities across the network. Because DABomb works in an automated fashion, it is frequently faster at parsing scan results and prioritizing attack vectors than a security analyst is when performing the same test manually.

Exploitation
Following the scanning phase, security analysts attempt to infiltrate the network by exploiting discovered vulnerabilities to escalate their access from no access to Domain Administrator on the network.

RiskSense analysts have focused DABomb’s exploitation techniques to incorporate the most common and easy-to-exploit vulnerabilities found in penetration testing reports. These common types of vulnerabilities, covered by DABomb, include, but are not limited to, the following:

- EternalBlue
- EternalChampion
- EternalSynergy
- EternalRomance
- MS08-067
- PSExec
- NetBIOS/LLMNR Poisoning
- Apache Tomcat Default Credentials
- Insecure Printer Software, Services, and Configuration

Table 1: Example of Exploits Integrated in DABomb

Once a security analyst selects an exploit and designates what hosts to test, DABomb tests that exploit on each selected host to attain domain administrator access. Once a security analyst obtains domain administrator access, the analyst can maneuver through the compromised target network.

Post-Exploitation
If a vulnerable host is successfully exploited and access to the host is achieved, security analysts perform a wide variety of post-exploitation tasks. These tasks include enumeration of Active Directory users and groups, extracting credentials from the host’s memory, privilege escalations, and more.

DABomb can conduct several automated post-exploitation tasks, searching hosts for information that may be useful in finding a path to a Domain Administrator’s credentials. This process can be time consuming for a security analyst, especially with larger networks. DABomb allows analysts to conduct these tests without concern for time.
DABomb's automated post-exploitation techniques help answer the questions companies undergoing penetration assessments ask when determining the damage that can be done because of an adversary gaining access to a vulnerable host: What credentials were security analysts able to discover? Is there valuable information such as PHI and PII that the security analyst can access? How much of an impact is an organization going to face if these hosts were exploited by a malicious entity?

**DABomb: How Does this Artificial Intelligence-Based Automated Exploitation Framework Optimize Tasks?**

It its current state, DABomb exists as a command line tool. DABomb works in parallel with the Metasploit Framework, as shown in Figure 3 above. On the left, DABomb prints real-time status updates about the state of its current tasks. On the right is the instance of the Metasploit Framework that DABomb is using. Security analysts can interact with the various sessions that DABomb creates on exploited hosts both while DABomb is running and after DABomb has finished and has exited.

DABomb allows security-minded professionals to conduct the programmatic elements of penetration testing, allowing security analysts to focus on tasks that require the specialized expertise that they bring to the table.

Security analysts have so many tools at their disposal already. Why should they use DABomb? One of the main benefits of DABomb is that it can automatically search for and actively target the most common vulnerabilities found on nearly all networks today. DABomb validates these vulnerabilities for security analysts, reducing the time analysts spend on easy vulnerabilities so that they can instead search for and exploit the intricate and higher difficulty vulnerabilities that may also lurk on a network.

Another benefit is that DABomb is a flexible tool with the ability to allow for the addition of new features, tools, and exploits. The flexibility of DABomb means that not only is it the automated tool of today, but also of tomorrow as new tools, features, and modules can easily be added just as new vulnerabilities are found.

**Moving Forward: Bringing DABomb to RiskSense Clients**

DABomb is an incredibly versatile tool, and RiskSense is working hard to improve its functionality in several ways. Benjamin Mixon-Baca, a Security Automation Prototype Developer at RiskSense Inc., was tasked in improving the overall functionality of DABomb. He has several improvements in the works. Since receiving the code from Nate, Ben has gone through and refactored (optimized) DABomb's code, increasing its stability.

**Additional Deployments**

Daniel Peterson, a cross-trained Security Analyst and Prototype Developer at RiskSense, has dockerized DABomb. This means that even less-specialized IT staff can deploy DABomb easily into their environments with minimal configuration.

**Web Interface**

In addition to DABomb's primary use as a command line tool, DABomb also has a web interface to increase the availability of DABomb to other users as well as IT staff and security analysts.
Instead of using the command line version (what is now becoming the back-end version of DABomb), Ben is constructing a web application interface, using REST API, for DABomb. This version will have a streamlined graphical user interface (GUI). Instead of having to type specific commands into DABomb, users will be able to use the GUI's form fields to customize their inputs into the application.

Even with the GUI in place, security analysts will still have access to the command line back end. Technical users may find the command line backend more comfortable to work with.

This design has the added ability to send data about the steps a security analyst has taken during an assessment where DABomb and its front end have been used. This data will then be used in concert with machine learning algorithms and artificial intelligence techniques to enhance DABomb's decision making and mold DABomb to behave similarly to human penetration testers.

**Remote Functionality**

In its current state, DABomb requires a security analyst to have all DABomb's tools and programs installed. Along with the planned implementation of the GUI, RiskSense plans on hosting these tools on a server and attaching these to the web application interface.

This implementation will allow security analysts and other users to run DABomb without requiring the tools and dependencies of DABomb to be installed on every machine they use. This implementation also prevents the analyst's system from becoming overburdened by the processing requirements of these penetration testing tools.

**More Integration Options**

RiskSense has lots of plans for DABomb. One plan includes incorporating DABomb into the RiskSense platform. RiskSense platform integration will allow clients to use DABomb to run various tests on their networks and import the results of DABomb's tests back into the platform. Once there, clients can use the RiskSense platform's numerous features to prioritize and streamline their remediation processes. While DABomb should not be used as a replacement for a penetration test, it can help organizations conduct small tests that will help them better understand their vulnerabilities and weaknesses.

In addition, DABomb's platform integration will allow DABomb to leverage client scanner data loaded in the platform to make intelligent decisions about which exploits are most likely to succeed in a given environment. Using scan data from the RiskSense platform in conjunction with CVE-to-vulnerability mapping, DABomb can prioritize the vulnerabilities which were found on the network, improving DABomb's efficiency and effectiveness.

**KOADIC Integration**

RiskSense developed an open source hacking tool called Koadic™ C3 or COM Command and Control. Koadic is best described as a Microsoft Windows post-exploitation tool, which, while containing such penetration testing rootkits as Metasploit Meterpreter and PowerShell Empire, performs most of its operations using the Microsoft Windows Script Host (JScript/VBScript), which is in turn coupled tightly to the core Microsoft Windows operating system.

Daniel Peterson has integrated Koadic into DABomb, further increasing the efficacy of DABomb's post-exploitation capabilities.

---

**Figure 3: KOADIC Overview**
DABomb: Bringing Cost-Effective Benefits to Organizations

DABomb is a powerful tool that generates cost savings and improves customer satisfaction quickly by increasing efficiency and reducing penetration test cycle-time. DABomb currently provides security analysts with the ability to optimize their penetration test assessments through automation, allowing these analysts to focus on more complex tasks that require human interface. Future implementations of DABomb will allow organizations to tackle low-hanging fruit and provide them with the tools to improve their network security.

About RiskSense

RiskSense is disrupting the cyber risk market with a Software-as-a-Service based platform that uses domain expertise and data in ways that are beyond human cognition to correlate your vulnerability data with threat intelligence and business impact to measure risk, provide early warning of weaponization, predict attacks and prioritize remediation. We are empowering our customers to reduce vulnerability fatigue, improve efficiency and quantify risk based on diagnostic and operational data.

The RiskSense Platform™ embodies the expertise and intimate knowledge gained from real world experience in defending critical networks from the world’s most dangerous cyber adversaries.

As part of a team that collaborated with the U.S. Department of Defense and U.S. Intelligence Community, RiskSense founders developed Computational Analysis of Cyber Terrorism against the U.S. (CACTUS), Support Vectors Intrusion Detection, Behavior Risk Analysis of Vicious Executables (BRAVE), and the Strike Team Program. By leveraging RiskSense cyber risk management solutions, organizations can significantly shorten time-to-remediation, increase operational efficiency, strengthen their security programs, improve cyber hygiene, heighten response readiness, reduce costs, and ultimately minimize cyber risks. For more information, please visit www.risksense.com or follow us on Twitter at @RiskSense.
DABomb
RiskSense’s Automated Exploitation Framework