Cymulate

The 3 Approaches of Breach & Attack Simulation Technologies

Introduction

Testing the cybersecurity posture of an organization or its cybersecurity resilience to cyberattacks, has come a long way. The demand for the latest and most comprehensive testing solutions continues to grow to counter the ever-increasing wave of cybercrime. Until recently, the information security professional's arsenal of security effectiveness testing tools has mainly consisted of vulnerability scanners and manual penetration testing. But that has changed since Breach & Attack Simulation (BAS) technology has become available.

There are currently several vendors providing BAS solutions that are gaining traction, as more and more professionals are jumping on the BAS bandwagon. But just like everything else in life, there is no single BAS approach, but rather, several approaches, each with its own set of capabilities, benefits, and drawbacks. That being said, it is important to remember that all BAS solutions are able to simulate threat actor's hostile activities with some level of automation. That's what makes them so effective.

In this paper, we take a closer look at the different categories of BAS solutions to make it easier for CISOs, CIOs and other security leaders and practitioners to understand and select the most appropriate BAS solution for their organization.

APPROACH 1
Agent-based
vulnerability scanning solutions

APPROACH 2
"Malicious"
traffic-based testing solutions

APPROACH 3
Blackbox
multi-vector testing solutions

Approach 1

Agent-based vulnerability scanning solutions

Vulnerability scanners have been around for a while. They enable checking for vulnerabilities that are known or have already been exploited by cybercriminals. A number of BAS vendors have taken this tool to the next level by providing it as an agent-based solution that covers internal network security. These solutions are the simplest form of BAS and are deployed and utilized inside an organization's LAN on several machines (such as VMs, PCs and physical servers).

The agents are distributed across any number of machines and utilize a database of known vulnerabilities to be tested during the assessment. These solutions scan for thousands of different security vulnerabilities in the organization's networks or host systems, identifying vulnerabilities which may expose specific machines.
At the end of a test, the exposed machines are mapped out, including a potential attack route between them, that could be exploited by a threat actor. At the end of the test, a report is generated that includes a list of vulnerabilities with the required patches that can be used to mitigate them.

These solutions focus only on what might happen if an organization's network was breached, they do not test the perimeter of the organization to see if the network can be breached. This poses a problem for professionals seeking to gain a full picture of their security stance.

Approach 2

"Malicious" traffic-based testing solutions

Standard security solutions monitor traffic, detect malicious packets, and then block or quarantine them, after which they alert the IT security staff. This second category of BAS solutions tests the organization's security solutions based on generating "malicious" traffic inside the organization's internal network. This is done by setting up a number of Virtual Machines inside the organization's network that serve as targets for the test, using a database of various attack scenarios.

These BAS solutions perform their assessments by sending attacks between each of these machines and then checking if the organization's IPS and SIEM, or other solutions, can pick up on this "malicious" traffic by detecting and/or blocking it and generating the appropriate alerts. These BAS solutions do not use production machines for their tests and focus on network traffic detection of attack methods or vulnerabilities and how they are perceived by specific security solutions.

Following a test, a report is generated listing alerts that were raised during the assessment. This provides the organization with an overview of events that were not detected and blocked by the IPS and SIEM solutions. It also provides a list of rules and alerts to be set to block such traffic in the future. Similar to the previous method, these solutions focus only on what would happen if the enterprise network were breached, and do not test the organization's perimeter security.

Approach 3

Blackbox multi-vector testing solutions

This category of BAS solutions consists of multi vector simulated attacks that allow organizations to detect vulnerabilities both in the enterprise perimeter and the internal network. These assessments come much closer to testing the cybersecurity posture of an organization as effectively and intelligently as a cybercriminal or malicious hacker would do.

Most of these BAS solutions are cloud-based and do not require complex use of hardware and virtual machines to launch the assessment. By implementing a lightweight agent on a workstation within the network, stable communication between itself and the BAS platform is enabled, allowing assessments to run in a safe manner, while collecting the results and updating the management console.
These assessments consist of multi-step tests utilizing distinct types of adversary attack tactics, techniques, and procedures (TTPs) and payloads to try and bypass the security solutions and controls in place both internal and external to the organization's LAN. These attacks are therefore as close to real life as possible and identify which security solutions fail to detect and block attacks and send corresponding alerts. The generated report covers the vulnerabilities and exposures found in the organization's security framework layer by layer from breaches at the perimeter all the way to those related to specific assets.

These BAS solutions may differ from each other in the level of automation they offer in simulating malicious activities by threat actors, but they all enable cybersecurity professionals to know the probability and impact of the different risks they face in advance, based on which preventive measures can be taken.

Cymulate

The Cymulate Approach

Cymulate belongs to the third BAS category, blackbox multi-vector testing solutions, and includes the following capabilities:

01 Takes less than one hour to set up and deploy

02 Simulates all phases of an attack, from pre-exploitation to post-exploitation, persistence and maintaining access

03 Runs tests continuously, periodically or on-demand

04 Runs tests continuously, periodically or on-demand

05 Validates both network and endpoint security controls, as well as simulates lateral movement

06 Delivers simulations that include the newest threats detected in the wild

07 Provides comprehensive reporting, including executive and technical briefs with recommendations for mitigation

About Cymulate

Cymulate was established with the vision of empowering security professionals to make better decisions faster, based on real-time data. Founded and led by an elite team of cyber researchers with world-class experience in offensive cyber solutions, Cymulate is determined to become the golden standard for security professionals and leaders to know, control, and optimize their cybersecurity posture end to end. Trusted by hundreds of companies worldwide, Cymulate constantly enhances its methods to prepare organizations for any attack scenario or campaign.
With Cymulate, organizations continuously measure security performance in real-time, shore up defenses, and assure operational effectiveness.
Measuring your cybersecurity performance is fundamental towards creating a more secure organization!

Contact us for a live demo, or get started with a free trial

Start Your Free Trial

Headquarters: Maze St 3, Tel Aviv 6578931, 7546302, Israel | +972 3 9030732 | info@cymulate.com