Exploring the Cymulate Edge

How Targeted Cyberattack Simulations Differ from Penetration Tests & Vulnerability Scanning

Table of Content

Glossary

APT | Advanced Persistent Attack

CISO | Chief Information Security Officer

GDPR | EU General Data Protection Regulation

NYCRR | New York Codes, Rules and Regulations

PCI-DSS | Payment Card Industry Data Security Standard

SIEM | Security Incident and Event Management

SOC | Security Operations Center

SOX | Sarbanes-Oxley Act of 2002

WAF | Web Application Firewall

01 | Introduction

Organizations of all shapes and sizes are fighting a war against threat actors. As we have seen in recent years, cyberattacks have become more sophisticated, which makes them harder to detect and mitigate.

Current methods that organizations (and their CISOs) mainly use to verify that their systems and data are protected, are vulnerability scans and penetration tests. The results are used for risk assessments that have become an integral part of mandatory provisions in various regulations (e.g. GDPR and NYCRR).

As explored below, vulnerability scans and penetration tests are useful for getting insight into the security posture of an organization at a specific moment in time. However,

they do not present the full picture of an organization's security posture; especially when it comes to more sophisticated, multi-vector attacks.

The most effective way for an organization to test its resilience against the growing wave of cybercrime, is to opt for targeted attack simulations that use multi-vector simulated attacks. These kinds of simulations are also known as Breach & Attack Simulations (BAS). Gartner has assert that, "Security testing is so challenging for technical professionals focused on security operations that many don't try it. Breach and attack simulation tools help make security postures more consistent and automated."

02 | Vulnerability Scans

Vulnerability scans are performed by an application that may either be proprietary or open source. This app checks for vulnerabilities that are already known to vendors and the industry, or for weaknesses that have already been exploited by cybercriminals. Thousands of different security vulnerabilities in networks or host systems are scanned, such as software bugs, missing operating system patches, vulnerable services, insecure default configurations, and web application vulnerabilities. The scans are used to assist automating the security auditing process of an organization's IT.

By scanning networks and websites for thousands of different security risks, vulnerability scans can automate security auditing and be a central part of an organization's IT security. The resulting list of vulnerabilities to be patched can be used to remediate them.

Benefits

Automated, can be scheduled, easy to use

Detects known vulnerabilities

Fast, capable of producing results within a few hours

Does not require any special expertise

The latest exploits are uploaded

Could be more cost effective than pen-testing

Ability to perform multiple scans simultaneously

Disadvantages

Lack of process overview. It provides only a snapshot, and does not give substantial insights

Cannot detect vulnerabilities that have not been mapped yet. The time between updates leaves organizations exposed

Produces a high rate of false positives (estimated at 30% - 60%)

It lacks an appropriate adversary model threat scenario

Uploads require internet connection

Meant for non-critical systems; far less for critical real-time systems.

Could put stress on the production environment which may result in downtime

⚠ A vulnerability scan can only find a known vulnerability or threat. Since mitigation only entails updating and patching the system, misconfiguration or misusage of the infrastructure and the security solutions will not be mitigated.

03 | **Manual Penetration Tests**

Manual penetration testing (or pen-testing) is conducted by human testers (in-house or outsourced to a 3rd party) who attempt to evaluate the security of an organization's infrastructure by safely exploiting vulnerabilities. Those vulnerabilities may be present in operating systems, services or applications,

resulting from faulty configuration, or caused by careless end-user behavior. In other words, the corporate network, applications, devices, and/or people are attacked to check if a hacker would be able to penetrate the organization. The tests also reveal how deep an attacker could penetrate and how much data could be stolen or exploited.

Benefits

Identifies weaknesses that
vulnerability scans do not detect

Identifies selected high-risk
weaknesses

The pen-tester can learn about
a new attack technique and test it
the very next day

The assessment report can be used
to mitigate weaknesses

Provides a training tool
for network security

Disadvantages

Success depends on the skill and
expertise of each individual tester

Does not identify all weaknesses that
threat actors exploit due to the limited
testing environment

The tester cannot perform all the attack
methods that he/she has learned during
previous years

It takes a long time (weeks, sometimes
even more than a month) to receive
the assessment report

Does not provide 360° insight, since
manual testing is unable to test all
aspects of the system (e.g. lines of code,
decompiled Assembly, web pages and
parameters, web services, etc.),
in contrast to automated tools

The results of manual pen-tests reflect
a specific point of time. Often, they are
not performed due to high costs

04 | Red Teaming

Targeted simulated attacks, also known as red teaming or attacker simulation, are gaining popularity - and for good reason. Letting you take a proactive approach, apart from identifying weaknesses in the organization's security posture, they can also provide valuable insights about your organization's ability to identify attacks in progress and remove them from the environment. Multi-step attacks are used to simulate various types of adversaries, and for identifying gaps in information security controls through simulation optimization.

Benefits

Mimics the tactics, techniques and procedures (TTPs) deployed by real attackers

Prepares for real world cyberattacks by executing simulated attacks for given threat scenarios

Proactive approach

More cost effective than manual testing

Detects unknown issues at unknown locations

Enables evaluating security operations / monitoring capabilities

Disadvantages

Simulations must be conducted regularly

Requires in-house or outside expertise

Extent of effectiveness may be difficult to assess by CISOs and IT teams due to lack of consistency between one engagement to another

Requires significant resources, wether outsourced or conducted in-house

Due to lack of end-to-end automation, exercises are difficult to repeat in a consistent manner

Diffucult to assess the impact of changes to the environment on posture and track security performance over time

05 | **The Cymulate Approach**

Cymulate's Breach & Attack Simulation (BAS) platform takes targeted simulation attacks one step further by measuring the organization's true preparedness to handle cybersecurity threats effectively. Using an offensive approach, Cymulate exposes critical vulnerabilities by simulating multi-vector cyberattacks from an attacker's perspective. This sophisticated plug & play platform simulates and tests attack vectors by impersonating hackers, state-sponsored threat actors, and even rogue insiders before an actual attack takes place and exploits any weaknesses. The SaaS simulations can be run on-demand at any time and from anywhere without impacting the users or infrastructure. With Cymulate's Red Team capabilities, organizations can continuously test their cybersecurity posture against cyberattacks, global cybercrime campaigns and targeted APTs.
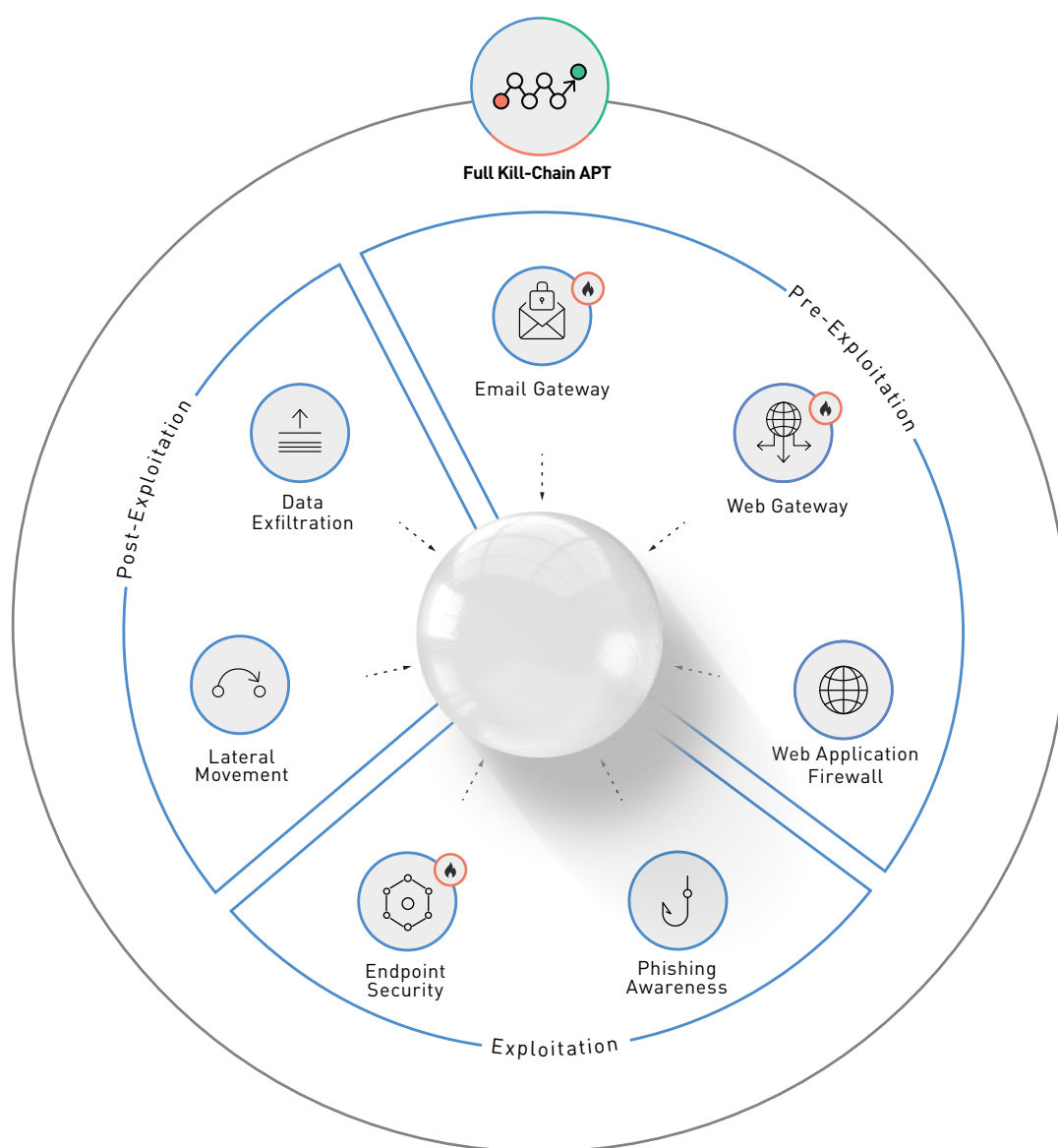

Figure 1 - Cymulate Attack Vectors Coverage

Features

Benefits

Pre-Exploitation

Immediate Threat
Test your organization's security posture against clear and present cyber danger

Continuous security validation against the very latest in-the-wild threats

Email Gateway
Test your organization's security posture against clear and present cyber danger

Simulates the broadest range of attack vectors in the industry, providing a comprehensive assessmen

Web Gateway
Test the organization's HTTP/HTTPS outbound exposure to malicious websites

Provides 360° insight pre- and post-exploitation and awareness

Web Application Firewall
Test the organization's HTTP/HTTPS outbound exposure to malicious websites

SaaS solution, no hardware required

Post-Exploitation

Data Exfiltration
Test the organization's outbound critical data safely before sensitive information is exposed

Immediate results 24x7x365

Lateral Movement
Test the organization's Windows domain network configuration using a sophisticated lateral movement algorithm

Mitigates attacks before they happen

Exploitation

Endpoint Security
Test if the organization's endpoint solutions are properly tuned to protect against the latest attack vectors

Excellent ROI and reduced TCO of the organization's cybersecurity investment

Phishing Awareness
Test employees' awareness of phishing campaigns with advanced, customizable simulations

Immediate results 24/7/365

Full Kill-Chain APT
Test the SOC team's incident response by launching pinpointed full Kill-Chain APT simulations

Fully automated and customizable blue-team exercises to assess effectiveness

06 | About Cymulate

Cymulate helps companies stay one step ahead of cyber attackers with a unique breach and attack simulation service that empowers organizations with complex security solutions to safeguard their business-critical assets. By mimicking the myriad strategies hackers deploy, the system allows businesses to assess their true preparedness to handle cyber security threats effectively.

Cymulate is trusted by companies worldwide, from small businesses to large enterprises, including leading banks and financial services. They share our vision—to make it easy for anyone to protect their company with the highest levels of security. Because the easier cybersecurity is, the more secure your company - and every company - will be.

For more information, visit www.cymulate.com
or contact us for a schedule a demo