Cyber Security Validation

How Targeted Cyber Attack Simulations Differ from Penetration Tests and Vulnerability Scanning

TABLE OF CONTENTS

GLOSSARY

APT	Advanced Persistent Attack
BAS	Breach and Attack Simulations
CISO	Chief Information Security Officer
GDPR	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 Centre
SOX	Sarbanes-Oxley Act of 2002
TTPs	Tactics, Techniques and Procedures
WAF	Web Application Firewall

INTRODUCTION

Organisations of all shapes and sizes are fighting the war against cyber attackers. As we have seen in recent years, cyber attacks are becoming more sophisticated which makes them harder to detect and mitigate. Current methods used by organisations to verify that their systems and data are protected include vulnerability scans and penetration tests.

The results generated from these tests are utilised for risk assessments, which have become an integral part of mandatory provisions in various regulations (e.g. GDPR and NYCRR). As we will see in this paper, vulnerability scans and penetration tests are useful for getting insight into the security posture of an organisation at a specific moment in time. However, although valuable, they do not present the full picture; especially when it comes to more sophisticated, multi-vector attacks.

The optimal way for an organisation to test its resilience against the growing cyber attack wave is to opt for targeted attack simulations that use multi-vector simulated attacks. These kinds of simulations are also known as Breach and Attack Simulations (BAS). During its July 2017 Hype Cycle (a graphical representation of how a technology or application will evolve), Gartner stated:

> *"The ability to provide continuous testing at limited risk is the key advantage of BAS technologies, which are used to alert IT and business stakeholders about existing gaps in the security posture, or validate that security infrastructure, configuration settings, and prevention technologies are operating as intended."*

VULNERABILITY SCANS

Vulnerability scans are performed by an application (proprietary or open source) and check for vulnerabilities that are already known to vendors, integrators and security experts, plus those that have already been exploited by cyber attackers.

The application scans for thousands of different security weaknesses in networks or host systems, such as software bugs, missing operating system patches, vulnerable services, insecure default configurations, and web application vulnerabilities.

Ultimately, these scans will give your IT systems and network administrators the data they need to keep your information safe and secure.

BENEFITS
Automated, can be scheduled, easy to use
Detects known vulnerabilities
Fast, able to produce results within hours
Does not require special expertise
Could be more cost-effective than penetration testing
The latest exploits are uploaded

DISADVANTAGES
Lack of process overview and provides only a snapshot, without substantial insights
Cannot identify vulnerabilities that have not been mapped yet. The time between updates leaves the organisation exposed
Generates a high rate of false positives (estimated at 30-60%)
Lacks an appropriate adversary model threat scenario
Meant for non-critical systems, not so much for critical real-time systems
Could put stress on production environment which may lead to downtime

MANUAL PENETRATION TESTING

Manual penetration testing (or pen-testing) is an authorised simulated cyber attack against your computer system to check for exploitable vulnerabilities and is conducted in-house or outsourced to a third-party.

Vulnerabilities can be present in computer systems, networks, applications and websites, as well as faulty configurations or careless end-user behaviour. Penetration testing will identify and address these vulnerabilities in order to mitigate the risk of suffering a malicious attack. The tests also reveal how far an attacker could go and how much data could be stolen or exploited.

BENEFITS
Identifies weaknesses that vulnerability scans do not detect
Identifies selected high-risk weaknesses
The penetration 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 the tester
Does not recognise all weaknesses that cyber attackers exploit due to the limited testing environment
The tester cannot perform all the attack methods that he/she has acquired during the last few years
It takes a long time (weeks, sometimes even more than a month) to receive the assessment report
Does not offer a 360-degree insight since manual testing is unable to test aspects of the system (e.g. lines of code, decompiled assembly, web pages and parameters, web services etc.) compared to automated tools

TARGETED SIMULATED ATTACKS

Targeted simulated attacks (also known as red teaming or attacker simulations) are gaining in popularity and for good reason. Apart from identifying weaknesses in the organisation's security posture, they can also provide valuable insight into your organisation's ability to detect attacks in action and remove them from the environment to take a proactive approach.

This approach uses multi-step attacks for distinct adversary types and leverages this knowledge to identify promising combinations of information security control through simulation optimisation.

BENEFITS
Mimics the tactics, techniques and procedures (TTPs) deployed by real attackers
Prepares for real-world cyber attacks by executing similar attacks for given threat scenarios
Proactive approach
More cost effective than manual testing
Detects unknown issues at unknown locations

DISADVANTAGES
Simulations must be conducted regularly
Requires in-house or outside expertise
Requires follow-up to mitigate risks
Needs to comply with the organisations security policy as mandated by various provisions in regulations
CIOs and IT teams do not always understand its effectiveness

THE APPROACH – BREACH & ATTACK SIMULATION

Breach & Attack Simulation (BAS) solutions take targeted simulation attacks one step further by measuring the organisation's true preparedness to handle cyber security risks effectively.

Using an offensive approach and defensive actions, breach and attack simulation exposes critical vulnerabilities by simulating multi-vector cyber attacks from an attacker's perspective. This sophisticated plug-and-play service simulates and tests attack vectors by impersonating attackers and even rogue insiders before an actual attack takes place, exploiting any weaknesses.

The SaaS simulations can be run on-demand at any time and from anywhere without impacting the users or infrastructure. With it's Red Team capabilities, organisations can continuously test their cyber security posture against cyber attacks and directed APTs.

Figure 1 – Breach and Attack Simulation Vectors Coverage

Pre-Exploitation

Immediate Threat

Features

Test your organisation's security posture against clear and present cyber danger.

Email Assessment

Features

Testing the organisation's entire email security flow using a wide range of diverse simulated email attacks.

Browsing Assessment

Features

Testing the organisation's HTTP/HTTPS outbound exposure to malicious websites.

Web Application Firewall Assessment

Features

Testing the organisation's WAF security posture to Web payloads (e.g. XSS or SQL Injection).

Post-Exploitation

Data Exfiltration Assessment

Features

Testing the organisation's outbound critical data safely before sensitive information is exposed.

Hopper (Lateral Movement)

Features

Testing the organisation's outbound critical data safely before sensitive information is exposed.

Endpoint Assessment

Features

Testing if the organisation's endpoint solutions are tuned correctly and if they are protecting the organisation against the latest attack vectors.

Awareness

Phishing Assessment

Features

Testing the employees' awareness of phishing campaigns with advanced simulations.

SIEM/SOC Simulation

Features

Testing the organisation's SOC team awareness using our intuitive GUI and attack correlations.

WHO ARE SECRUTINY?

We are Incident Response specialists who spend 95% of our time making sure our clients don't need to respond to incidents. Secrutiny was founded by three people – all veterans who came to realise there is much confusion in the industry... tools were often overly complex, misconfigured and isolated, and adding further 'layers to the security onion' at significant cost was not the answer.

Through responding to 300+ incidents, we learnt the way to help organisations NOT to be breached is to support them in achieving better security and risk reduction with what they already have; adding capability, where necessary, based on evidence and risk appetite.

We're here to answer any questions you may have and always happy to share our experiences. Reach out to us and we'll respond as soon as we can.

www.secrutiny.com

enquiries@secrutiny.com

0203 8232 999