BREACH AND ATTACK SIMULATION VS PEN TESTING

By Gus Evangelakos, Director Field Engineering, XM Cyber

How easy is it for a malicious actor to get into your network? Cyber attacks are growing steadily in number, strength, and variety. In parallel, even the most sophisticated adversaries are using surprisingly unsophisticated means to wreak damage.

Top-notch hackers can mimic legitimate user actions and go under the radar of protective measures. They can move laterally from hole to hole and reach what matters most to you – your crown jewels. Therefore, a large number of organizations are coming to see that a proactive security strategy is one of the best defenses.

Simply put, you need to see where the threats are coming from, how they can move within your network, where the vulnerabilities in your defenses are, find them and close them before cyber attackers take advantage of them.

Let's take a look at some options that are available today.

PENETRATION TESTING AND RED TEAM ASSESSMENT

Many people find it particularly challenging to understand the difference between the terms "penetration testing" and "red teaming". Let's learn from IBM's SecurityIntelligence article titled Penetration Testing Versus Red Teaming: Clearing the Confusion.

"Penetration Testing is a manual testing typically conducted independently of a vulnerability assessment and used to help test the effectiveness of an organization's vulnerability management program and associated controls within a defined scope. Pen tests are used to test whether certain networks, assets, platforms, hardware or applications are vulnerable to an attacker. Penetration tests are not focused on stealth, evasion, or the ability of the blue team to detect and respond, since the blue team is fully aware of the scope of the testing being conducted.

Similar to scenario-based penetration tests, Red Team engagements are designed to achieve specific goals, such as gaining access to a sensitive server or business-critical application. Red teaming projects differ in that they are heavily focused on emulating an advanced threat actor using stealth, subverting established defensive controls and identifying gaps in the organization's defensive strategy. The value of this type of engagement can be derived from a better understanding of how an organization detects and responds to real-world attacks."

Pen testing can overlap with red team exercises and this may be a bit confusing to some people. It turns out that pen testers and red teams can be the same people, using different methods and techniques for different assessments. They are like judo and karate, or sumo and krav maga – one is not necessarily better than the other and organizations see value in both.

WELCOME TO BREACH AND ATTACK SIMULATION (BAS)

Recently, a new category of solutions has emerged to add some spice to the matter. Breach and Attack Simulation (BAS) solutions represent a new and emerging market and are directly adjacent to vulnerability assessment, according to the Market Guide for Vulnerability Assessment.

They perform automated security testing: some challenge the existing security infrastructure and some model attack chains to identify the most-likely path an attacker would use to compromise an environment. BAS products are becoming more mainstream and have begun transforming the security testing landscape.

BAS VS. PEN TESTING

There seems to be some confusion around the definition of BAS and its relationship to penetration testing. An easy way to clarify the idea is to highlight some major advantages of the former over the latter:

Simulation vs. Real Attack: Cybersecurity resembles a military drill, where only the latest proactive practices and processes will keep you from defeat. The military keeps their soldiers on their toes by continuously running wargames; cybersecurity experts should be doing the same by running simulated cyber-attacks, which will show you attack paths and weaknesses in your IT systems and your network. BAS tools allow organizations to continually and safely simulate the realistic full attack cycle against their infrastructure, virtual machines, and other means.

Automated vs. Human-Led: Penetration testing is conducted by security experts, ethical "white hat hackers" who apply their knowledge of how to breach defenses to the task of penetrating an organization's networks. BAS tools automate the testing process, performing the cycle of scan, exploit and repeat. "If this can now be done with the simple click of a button, why would you use a human to do it? The tools can ensure consistency, provide better reporting and do the work faster", said Gartner's research VP Augusto Barros. "These tools provide a lot of insight on security holes and can greatly decrease the manual effort required during testing," SC Magazine wrote.

Continuous vs. One Point in Time: A pen test offers a snapshot of an organization's defenses at a specific point in time. Not only does BAS automate the testing process, but it also performs it continuously. BAS is exactly the solution for testing all the time across a broad spectrum of different kinds of attacks and helping identify vulnerabilities as changes happen in your network. Therefore, the organization can know its security posture at any given time and know how to focus its resources on the most critical issues.

"Penetration testing helps answer the question 'can they get in?'; BAS tools answer the question 'does my security work?'," Gartner's research VP and analyst Anton Chuvakin summarized. XM Cyber goes one step beyond and addresses the only crucial question for enterprises: "are my critical assets really secure?"

PURPLE TEAM: AUTOMATION + REMEDIATION SOLUTION

HaXM by XM Cyber is the first BAS platform to simulate, validate and remediate attackers' paths to your critical assets 24×7. HaXM's automated purple teaming aligns red and blue teams to provide the full realistic APT experience on one hand while delivering vital prioritized remediation on the other. Addressing real user behavior and exploits, the full spectrum of scenarios is aligned to your organization's own network to expose blind spots and is executed using the most up-to-date attack techniques safely, without affecting network availability and user experience.

The move to automation empowers organizations with the ability to gain a worm's eye view into new back doors and blind spots as soon as they appear and move to remediate them immediately without delay.

Will Breach and Attack Simulation and Red Teams Kill the Pen Test? Gartner's Barros has raised an interesting discussion about the role of the pen test, which he believes will cease to exist.

“Simple pen testing, for pure vulnerability finding goals and with no intent to replicate threat behavior, will vanish. This is different from the pen test that many people will prefer to call ‘red team exercises’, those very high-quality exercises where you really try to replicate the approach and methods of real threats. That approach is in fact growing, and that growth is one of the factors that will kill the vanilla pen test,” he wrote.

“BAS automates the simple pen test, performing the basic cycle of scan/exploit/repeat-until-everything-is-owned. If you have the ability to do that with a simple click of a button, why would you use a human to do that? The tool can ensure consistency, provide better reporting and do it faster. Not to mention requiring fewer skills,” he added.

“Top-notch hackers can mimic legitimate user actions and go under the radar of protective measures. They can move laterally from hole to hole and reach what matters most to you – your crown jewels.”

ABOUT XM CYBER

XM Cyber was founded by security executives from the elite Israeli intelligence sector.

XM Cyber’s core team is comprised of highly skilled and experienced veterans from the Israeli Intelligence with expertise in both offensive and defensive cyber security.

XM Cyber has developed more than 15 patented technologies based on a proprietary set of algorithms that enable the continuous and automatic simulation of a hacker’s techniques and methods.

GUS EVANGELAKOS

is the Director of North American Field Engineering, at XM Cyber. He has extensive experience in cyber security, having managed implementations and customer success for manymajor global brands such as Varonis, Bromium and Comodo. Gus has spent a decade also working on the client side, supporting IT infrastructure and cybersecurity projects. He has a strong background in micro virtualization, machine learning, deep learning (AI), sandboxing, containment, HIPS, AV, behavioral analysis, IOCs, and threat intelligence.